Docket No.: 070456-0056 **PATENT**

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of	:	Customer Number: 20277
	:	
Yoshihiro HORI, et al.	:	Confirmation Number: 2825
	:	
Application No.: 10/506,505	:	Group Art Unit: 2131
	:	
Filed: September 03, 2004	:	Examiner: Christian A. Laforgia
	:	

For: DATA STORING DEVICE FOR CLASSIFIED DATA (AS AMENDED)

SUBMISSION OF CERTIFIED TRANSLATION OF PRIORITY DOCUMENT

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This application is entitled to have the benefit of earlier filing date of March 5, 2002, based on Japanese Patent Application No. 2002-59179, pursuant to 35 U.S.C. §119. Applicants submit a certified English language translation of Japanese Application No. 2002-59179.

Respectfully submitted,

McDERMOTT WILL & EMERY LLP

Tomoki Tanida
Registration No. 60,453

600 13th Street, N.W.
Washington, DC 20005-3096
Phone: 202.756.8000 SAB:TT:lnm
Facsimile: 202.756.8087
Date: July 17, 2007

Please recognize our Customer No. 20277 as our correspondence address.

WDC99 1424561-1.070456.0056

DECLARATION

I, Yutaka Horii, c/o Fukami Patent Office, Nakanoshima Central Tower, 22nd Floor, 2-7, Nakanoshima 2-chome, Kita-ku, Osaka-shi, Osaka, Japan, declare:

that I know well both the Japanese and English languages;

that to the best of my knowledge and belief the English translation attached hereto is a true and correct translation of Japanese Patent Application No. 2002-059179, filed on March 5, 2002;

that all statements made of my own knowledge are true;

that all statements made on information and belief are believed to be true; and

that the statements are made with the knowledge that willful false statements and the like are punishable by fine or imprisonment, or both, under 18 USC 1001.

Dated: July 12, 2007

Yutaka Horii

[Document Name]	Petition for Patent
[Reference Number]	1020002
[Filing Date]	March 5, 2002
[Destination]	To the Commissioner of the JPO
[International Class]	H04M 11/08
[Inventor]	
[Address]	c/o Sanyo Electric Co., Ltd., 5-5, Keihanhondori 2-chome, Moriguchi-shi, Osaka
[Name]	Yoshihiro HORI
[Inventor]	
[Address]	c/o Sharp Kabushiki Kaisha, 22-22, Nagaike-cho, Abeno-ku, Osaka-shi, Osaka
[Name]	Ryoji OHNO
[Inventor]	
[Address]	c/o Victor Company of Japan, Limited, 12, Moriya-cho 3-chome, Kanagawa-ku, Yokohama-shi, Kanagawa
[Name]	Takeo OHISHI
[Inventor]	
[Address]	c/o Tokorozawa Works of Pioneer Corporation, 2610, Hanazono 4-chome, Tokorozawa-shi, Saitama
[Name]	Kenichiro TADA
[Inventor]	
[Address]	c/o Systems Development Laboratory, Hitachi, Ltd., 1099, Ozenji, Asao-ku Kawasaki-shi, Kanagawa
[Name]	Tatsuya HIRAI

[Inventor]	
[Address]	c/o Phoenix Technologies, K.K. Shinjuku Kofu Building 6th Floor, 2-18, Shinjuku 4-chome, Shinjuku-ku, Tokyo
[Name]	Masafumi TSURU
[Inventor]	
[Address]	c/o Fujitsu Limited, 1-1, Kamikodanaka 4-chome, Nakahara-ku, Kawasaki-shi, Kanagawa
[Name]	Takayuki HASEBE
[Applicant]	
[Identification Number]	000001889
[Address]	5-5, Keihanhondori 2-chome, Moriguchi-shi, Osaka
[Name]	Sanyo Electric Co., Ltd.
[Applicant]	
[Identification Number]	000005049
[Address]	22-22, Nagaike-cho, Abeno-ku, Osaka-shi, Osaka
[Name]	Sharp Kabushiki Kaisha
[Applicant]	
[Identification Number]	000004329
[Address]	12, Moriya-cho 3-chome, Kanagawa-ku, Yokohama-shi, Kanagawa
[Name]	Victor Company of Japan, Limited
[Applicant]	
[Identification Number]	000005016
[Address]	4-1, Meguro 1-chome, Meguro-ku, Tokyo

[Name]	Pioneer Corporation
[Applicant]	
[Identification Number]	000005108
[Address]	6, Kandasurugadai 4-chome, Chiyoda-ku, Tokyo
[Name]	Hitachi, Ltd.
[Applicant]	
[Identification Number]	300017636
[Address]	Shinjuku Kofu Building 6th Floor, 2-18, Shinjuku 4-chome, Shinjuku-ku, Tokyo
[Name]	Phoenix Technologies, K.K.
[Applicant]	
[Identification Number]	000005223
[Address]	1-1, Kamikodanaka 4-chome, Nakahara-ku, Kawasaki-shi, Kanagawa
[Name]	Fujitsu Limited
[Attorney]	
[Identification Number]	100064746
[Patent Attorney]	
[Name]	Hisao FUKAMI
[Appointed Attorney]	
[Identification Number]	100085132
[Patent Attorney]	
[Name]	Toshio MORITA
[Appointed Attorney]	
[Identification Number]	100091409

[Patent Attorney]		
[Name]	Hidehiko ITOH	
[Appointed Attorney]		
[Identification Number]	100096781	
[Patent Attorney]		
[Name]	Yutaka HORII	
[Indication of Fee]		
[Deposit Account Number]	008693	
[Fee]	21000	
[List of the Accompanying Documents]		
[Document]	Specification	1
[Document]	Drawings	1
[Document]	Abstract	1

[Document Name] Specification

[Title of the Invention] Data Storage Device

[Scope of Claims for Patent]

[Claim 1] A data storage device performing input/output of classified data in accordance with predetermined input/output procedures for protection of said classified data, and storing said classified data, comprising:

interface means for externally exchanging data;

first storage means for storing said classified data; and

second storage means for storing log information related to the input/output of said classified data according to said predetermined input/output procedures and an address representing a storage position of said classified data to be input/output in said first storage means.

[Claim 2] The data storage device according to claim 1, further comprising control means for controlling the input/output of said classified data, wherein

said log information includes:

an identification code identifying said classified data to be input/output; and

a first status representing a state of storage of said classified data to be input/output in said first storage means, and

said control means operates in accordance with said predetermined input/output procedures to receive said identification code and said address of said classified data to be input/output via said interface means, and to store said identification code and said address in said second storage means, and operates in response to a request that is externally applied via said interface means to determine the state of storage of said classified data in said first storage means, based on said identification code and said address stored in said second storage means, and to renew said first status based on said state of storage.

[Claim 3] The data storage device according to claim 2, wherein

said log information further includes a second status recording a status of progression of said predetermined input/output procedures relating to the input/output of said classified data to be input/output, and

said control means renews said second status in accordance with the progression of said predetermined input/output procedures.

[Claim 4] The data storage device according to claim 2 or 3, wherein

said log information further includes procedure specifying information specifying said predetermined input/output procedures, and

said control means renews said procedure specifying information every time said procedure specifying information is newly obtained.

[Claim 5] The data storage device according to any one of claims 2 to 4, wherein

said classified data includes said identification code peculiar to the classified data, and

said control means determines the state of storage of said classified data in said first storage means by specifying said classified data in accordance with said identification code included in said classified data stored at the storage position on said first storage means specified by said address.

[Claim 6] The data storage device according to claim 5, wherein

in an input procedure for receiving said classified data via said interface means and storing said classified data in said first storage means, said control means stops said input procedure without storing said classified data in said first storage means when mismatch occurs between the identification code included in said received classified data and the identification code included in said log information.

[Claim 7] The data storage device according to claim 5 or 6, wherein

in an output procedure for outputting said classified data stored in said first storage means via said interface means, said control means stops said output procedure without outputting said classified data when mismatch occurs between the identification code included in said classified data stored at the storage position on said first storage means specified by said address and the identification code included in said log information.

[Claim 8] The data storage device according to any one of claims 2 to 7, further comprising signing means for producing signed data for said log information and producing signed log information by affixing said produced signed data to said log information, wherein

in a re-input procedure performed for resuming an input procedure when the input procedure for receiving said classified data via said interface means and storing said classified data in said first storage means is interrupted, said control means outputs said signed log information produced by said signing means via said interface means.

[Claim 9] The data storage device according to claim 8, further comprising log certifying means for verifying and certifying correctness of additional signed log information prepared by affixing signed data for additional log information of a receiver of said classified data to the additional log information, and received from said receiver of said classified data via said interface means, wherein

in a re-output procedure performed for resuming an output procedure when the output procedure for outputting said classified data stored in said first storage means via said interface means is interrupted, said log certifying means verifies correctness of said additional signed log information received from the receiver of said classified data in said interrupted output procedure and,

when it is determined that said additional signed log information is not correct, or when the correctness of said additional signed log information is certified and it is determined based on said additional signed log information and said log information stored in said second storage means that said output procedure is not interrupted, said control means stops said re-output procedure.

[Claim 10] The data storage device according to claim 4, further comprising certificate holding means for holding a certificate to be output to a supplier of said classified data, wherein when an input procedure is started for receiving said classified data via said interface means and storing said classified data in said first storage means, said control means outputs said certificate via said interface means in response to a request to output said certificate received via said interface means and, when said supplier certifies said certificate, said control means receives said classified data from said supplier via said interface means.

[Claim 11] The data storage device according to claim 10, wherein

said certificate includes a public key associated with said data storage device, and

said data storage device further comprises:

private key holding means for holding a private key for decrypting data encrypted by said public key;

first decrypting means using said private key for decrypting the data encrypted by said public key;

session key generating means for generating a first session key peculiar to said predetermined input/output procedures in said predetermined input/output procedures for performing input/output of said classified data;

encrypting means for encrypting data by a second session key generated by said supplier; and

second decrypting means for decrypting data encrypted by said first session key,

in said input procedure,

said session key generating means generates said first session key,

said first decrypting means uses said private key to decrypt said second session key encrypted by said public key,

said encrypting means encrypts said first session key by said second session key received from said first decrypting means,

said second decrypting means uses said first session key to decrypt said classified data encrypted by said first session key, said control means provides to said first decrypting means said second session key encrypted by said public key received from said supplier via said interface means, outputs said first session key encrypted by said second session key for providing said first session key via said interface means to said supplier, provides to said second decrypting means said classified data encrypted by said first session key received from said supplier via said interface means, and stores said classified data as decrypted, at a storage position on said first storage means specified by said address.

[Claim 12] The data storage device according to claim 11, wherein

said procedure specifying information is said first session key for specifying said input procedure, and

said control means renews said procedure specifying information every time said first session key is generated by said session key generating means.

[Claim 13] The data storage device according to claim 11 or 12, further comprising signing means for producing signed data for said log information that can be certified by said second session key received from said first decrypting means, and producing signed log information by affixing said produced signed data to said log information, wherein

in a re-input procedure for resuming said input procedure when said input procedure is interrupted,

said first decrypting means decrypts said second session key encrypted by said public key newly received from said supplier via said interface means,

said signing means produces said signed log information by newly received said second session key, after said first status stored in said second storage means is renewed, and

said control means provides to said first decrypting means said second session key encrypted by said public key newly received from said supplier via said interface means, renews said first status, and outputs said signed log information produced by said signing means for providing said signed log information via said interface means to said supplier.

[Claim 14] The data storage device according to any one of claims 10 to 13, wherein

said classified data includes said identification code peculiar to the classified data, and

said control means specifies said classified data by said identification code included in said classified data stored at a storage position on said first storage means specified by said address, when the state of storage of said classified data in said first storage means is determined.

[Claim 15] The data storage device according to claim 14, wherein

said control means stops storage of said classified data in said first storage means when mismatch occurs between the identification code included in said received classified data and the identification code included in said log information.

[Claim 16] The data storage device according to claim 10, further comprising certifying means for verifying and certifying correctness of an additional certificate of a receiver to which said classified data stored in said first storage means is to be supplied, said additional certificate being received from said receiver, wherein

in an output procedure for outputting said classified data via said interface means,

said certifying means verifies said additional certificate received from said receiver, and

said control means provides to said certifying means said additional certificate received from said receiver via said interface means and, when said additional certificate is not certified by said certifying means, said control means stops said output procedure.

[Claim 17] The data storage device according to any one of claims 11 to 13, further comprising:

certifying means for verifying and certifying correctness of an additional certificate of a receiver to which said classified data stored in said first storage means is to be supplied, said additional certificate being received from said receiver; and additional encrypting means for encrypting data by a public key associated with said receiver that is included in said additional certificate, wherein

in an output procedure for outputting said classified data via said interface means,

said certifying means certifies said additional certificate received from said receiver,

said session key generating means further generates a third session key,

said additional encrypting means uses the public key associated with said receiver to encrypt said third session key,

said second decrypting means uses said third session key to further decrypt a fourth session key generated by said receiver that is encrypted by said third session key,

said encrypting means uses said fourth session key received from said second decrypting means to further encrypt said classified data, and

said control means provides to said certifying means said additional certificate received from said receiver via said interface means and, when said certifying means certifies said additional certificate, said control means provides to said additional encrypting means the public key associated with said receiver that is included in said additional certificate, outputs said third session key encrypted by the public key associated with said receiver for providing said third session key to said receiver via said interface means, provides to said second decrypting means said fourth session key encrypted by said third session key received from said receiver via said interface means, obtains said classified data stored at a storage position on said first storage means specified by said address and provides the obtained classified data to said encrypting means, and outputs said classified data encrypted by said fourth session key for providing said classified data to said receiver via said interface means.

[Claim 18] The data storage device according to claim 17, wherein

said procedure specifying information is said fourth session key specifying said output procedure, and

said control means renews said procedure specifying information every time said fourth session key is decrypted that is encrypted with said third session key, by said second decrypting means.

[Claim 19] The data storage device according to any one of claims 16 to 18, wherein

said classified data includes said identification code peculiar to the classified data, and

said control means stops said output procedure without outputting said classified data when mismatch occurs between said identification code included in said classified data stored at a storage position on said first storage means specified by said address and the identification code included in said log information.

[Claim 20] The data storage device according to claim 16, further comprising log certifying means for verifying and certifying correctness of signed log information prepared by affixing signed data for additional log information of a receiver of said classified data to said additional log information, and received from said receiver of said classified data via said interface means, wherein

in a re-output procedure for resuming an output procedure when the output procedure for outputting said classified data stored in said first storage means via said interface means is interrupted,

said log certifying means verifies correctness of said signed log information received from the receiver of said classified data in said interrupted output procedure, and

said control means stops said re-output procedure, when it is determined that said signed log information not correct, or when the correctness of said signed log information is certified and it is determined based on said signed log information and said log information stored in said second storage means of said data storage device that said output procedure is not interrupted.

[Claim 21] The data storage device according to claim 17 or 18, further comprising log certifying means for verifying and certifying correctness of additional signed log information having a sign given to additional log information of a receiver of said classified data by said fourth session key, as received from said receiver via said interface means, wherein

in a re-output procedure for resuming an output procedure when the output procedure for outputting said classified data stored in said first storage means via said interface means is interrupted,

said log certifying means verifies correctness of said additional signed log information received from the receiver of said classified data in said interrupted output procedure, and

when it is determined that said additional signed log information is not correct or when the correctness of said additional signed log information is certified and it is determined that said output procedure is not interrupted based on said additional signed log information and said log information stored in said second storage means of said data storage device, said control means stops said re-output procedure.

[Claim 22] The data storage device according to any one of claims 1 to 21, wherein

said classified data is a decryption key for decrypting and using encrypted content data, and

said data storage device further comprises third storage means for storing said encrypted content data.

[Claim 23] The data storage device according to claim 22, wherein

said third storage means is a hard disk.

[Detailed Description of the Invention]

[Technical Field to Which the Invention Belongs]

The present invention relates to a data storage device in a data distributing system, which allows copyright protection of content data in a digital form, and particularly to a data storage device, which can safely input/output licenses (decryption keys and usage rules) required for reproducing encrypted content data prepared by encrypting content data, can store many licenses, can safely input/output classified data requiring protection, and can safely resume the input/output of interrupted input/output of the classified data.

[Prior Art]

Owing to progress in digital information communication networks and the like such as the Internet in recent years, users of personal terminals can easily access network information.

In such digital information communication networks, information is transmitted by digital signals. Even an individual user can copy music or movie data transmitted via the aforementioned information network for example, and thereby can copy such data without degrading audio and/or image qualities due to the copy.

Therefore, the copyright of the owner may be significantly infringed unless appropriate measures are taken for copyright protection when a copyrighted content such as music data or image data is transmitted over the digital information communication network.

However, if copyright protection is given top priority, it may become impossible to distribute content data over the fast-growing digital information communication network. This impairs an interest of the copyright owner, who can essentially collect predetermined copyright royalties for copy of the content data.

Instead of the distribution over the digital information communication network described above, distribution may be performed via record media storing digital data. In connection with the latter case, music data recorded on CDs (compact disks) on the market can be freely copied in principle onto magneto-optical disks (e.g., MDs) as long as copies are made only for the personal use. However, personal users performing digital recording or the like indirectly pay predetermined amounts in prices of digital recording devices or media such as MDs as guaranty moneys to copyright owners.

In view of the fact that the music data copied from a CD to an MD is digital data, which does not substantially cause copy deterioration, devices and others are configured for copyright protection to prohibit further copying of the copied music data as digital data from the recordable MD to another MD.

In connection with the above, the public distribution itself of the content data such as music data and image data over the digital information communication network is restricted by the public transmission right of the copyright owner, and therefore sufficient measures must be taken for the copyright protection in such distribution.

In the above case, it is necessary to prohibit unauthorized further copying of the content data such as music data or image data, which was a production once sent to the public over the digital information communication network.

A data distribution system has been proposed for distributing encrypted content data over a digital information communication network. In this data distribution system, a distribution server which holds encrypted content data generated by encrypting content data distributes the content data to memory cards, which are data storage devices attached to terminal devices such as cellular phones. In this data distribution system, a public encryption key of the memory card, which is already certified by a certification authority, and its certificate are sent to the distribution server when requesting the distribution of the encrypted content data. After the distribution server confirms the reception of the certified certificate, the encrypted content data and a content key for decrypting the encrypted content data are sent to the memory card. When distributing the encrypted content data and the content key, the distribution server and the memory card generate session keys, which are different from those generated for other distribution processes. With the session keys thus generated, the public encryption keys are encrypted, and the keys are exchanged between the distribution server and the memory card.

Finally, the distribution server sends the license, which is encrypted with the public encryption key peculiar to each memory card, and is further encrypted with the session key, as well as the encrypted content data to the memory card. The memory card stores the received content key and the encrypted content data in the memory.

When the encrypted content data stored in the memory card is to be reproduced, the user connects the memory card to the reproduction terminal provided with a dedicated reproducing circuit, and thereby can reproduce the encrypted content data for enjoying it.

In the above system, usage rules are determined so that a content supplier or a copyright owner can instruct a manner of use in connection with reproduction and copying of the encrypted content data. The rules thus determined are distributed together with the content key so that each device can perform processing according to the usage rules.

The usage rules define rules relating to copy/shift of the license between memory cards, rules such as restrictions on allowed times of reproduction in connection with output of the content key from the memory card, and rules relating to handling of reproduced contents.

[Problems to be Solved by the Invention]

In the data distribution system described above, the encrypted content data and the license concerning decode and use of encrypted content data are transmitted, e.g., between the distribution server and the data storage device or between the data storage device and the reproduction terminal. License generally represents the content key for decoding encrypted content data, license ID for identifying the license for the content or usage rules of contents already described. Such licenses are to be transmitted while ensuring sufficient security for the purpose of copyright protection.

In an operation of transmitting the license between devices, when ordinary transmission processing is being performed, the sender and the receiver mutually recognize the transmitted licenses, respectively, so that the license can be transmitted between the devices without any problem. However, when a failure (such as power-down of the device for example) occurs in either of the devices or a communication path during the transmission of the license, the license may be lost during the transmission.

For the processing of, e.g., transmitting the license between the data storage devices, the system is configured to prevent such a state that both the data storage devices on the sender and receiver sides can simultaneously utilize the same license when storing the data, in view of the copyright protection, except for the case where the usage rules permit the copying of the license of free contents. Thus, the license stored in the data storage device on the sender side must be configured to become unavailable at the same time as the output of the license to the data storage device on the receiver side. In this configuration, such a state temporarily occurs that neither of the data storage devices has stored the license in an available state. When the transmission processing is interrupted due to a failure during the above case, the license, which is being transmitted, is lost. In the operation of receiving the license from the distribution server, the license may likewise be lost. In the case where the transmission of the license is interrupted, it is therefore important to specify the interrupted transmission and the license to know the storage state of the specified license, and to perform retransmission of the lost license in the optimum manner if the license was lost. In the data storage device, information for specifying again the interrupted transmission processing and the license must be stored efficiently.

It can be reliably considered that the information transmission technology, which has been remarkably progressed in recent years, will further progress, and such progress will result in increase in information amount, information in multimedia form, further advance in communication technology, and mass storage of the data storage device resulting from the progress in memory technology. For these reasons, it is expected that a data storage device in the data distribution system stores various kinds of and a large number of content data.

In this case, the mass storage data storage device stores a considerable number of content data and accordingly hold licenses corresponding to respective content data. In this case, if a failure occurs while the license is transmitted in the data distribution system, it takes considerable time to retrieve and specify again the transmitted license from the considerable number of licenses as stored. The time is longer as the umber of stored licenses is larger.

According to a conventional system, in such a case, the retrieval processing must be effected for all licenses one by one for specifying the license, and the time required for the retrieval processing may cause a problem.

Accordingly, the invention has been developed for overcoming the above problems, and an object of the invention is to provide a data storage device which can rapidly specify a license being transmitted among a considerable number of stored licenses, and accomplish both of license protection and increased speed of reprocessing in the case where a failure occurs while the license is transmitted.

[Means for Solving the Problems]

According to the present invention, a data storage device performs input/output of classified data in accordance with predetermined input/output procedures for protection of the classified data, and stores the classified data. The data storage device includes: interface means for externally exchanging data; first storage means for storing the classified data; and second storage means for storing log information related to the input/output of the classified data according to the predetermined input/output procedures and an address representing a storage position of the classified data to be input/output in the first storage means.

Preferably, the data storage device further includes control means for controlling the input/output of the classified data, and the log information includes: an identification code identifying the classified data to be input/output; and a first status representing a state of storage of the classified data to be input/output in the first storage means. The control means operates in accordance with the predetermined input/output procedures to receive the identification code and the address of the classified data to be input/output via the interface means, and to store the identification code and the address in the second storage means, and operates in response to a request externally applied via the interface means to determine the state of storage of the classified data in the first storage means based on the identification code and the address stored in the second storage means, and to renew the first status based on the state of storage.

Preferably, the log information further includes a second status recording a status of progression of the predetermined input/output procedures relating to the input/output of the classified data to be input/output, and the control means renews the second status in accordance with the progression of the predetermined input/output procedures.

Preferably, the log information further includes procedure specifying information specifying the predetermined input/output procedures, and the control means renews the procedure specifying information every time the procedure specifying information is newly obtained.

Preferably, the classified data includes the identification code peculiar to the classified data, and the control means determines the state of storage of the classified data in the first storage means by specifying the classified data in accordance with the identification code included in the classified data stored at the storage position on the first storage means specified by the address.

Preferably, in an input procedure for receiving the classified data via the interface means and storing the classified data in the first storage means, the control means stops the input procedure without storing the classified data in the first storage means when mismatch occurs between the identification code included in the received classified data and the identification code included in the log information.

Preferably, in an output procedure for outputting the classified data stored in the first storage means via the interface means, the control means stops the output procedure without outputting the classified data when mismatch occurs between the identification code included in the classified data stored at the storage position on the first storage means specified by the address and the identification code included in the log information.

Preferably, the data storage device further includes signing means for producing signed data for the log information and producing signed log information by affixing the produced signed data to the log information. In a re-input procedure performed for resuming an input procedure when the input procedure for receiving the classified data via the interface means and storing the classified data in the first storage means is interrupted, the control means outputs the signed log information produced by the signing means via the interface means.

Preferably, the data storage device further includes log certifying means for verifying and certifying correctness of additional signed log information prepared by affixing signed data for additional log information of a receiver of the classified data to the additional log information, and received from the receiver of the classified data via the interface means. In a re-output procedure performed for resuming an output procedure when the output procedure for outputting the classified data stored in the first storage means via the interface means is interrupted, the log certifying means verifies correctness of the additional signed log information received from the receiver of the classified data in the interrupted output procedure. When it is determined that the additional signed log information is not correct, or when the correctness of the additional signed log information is certified and it is determined based on the additional signed log information and the log information stored in the second storage means that the output procedure is not interrupted, the control means stops the re-output procedure.

Preferably, the data storage device further includes certificate holding means for holding a certificate to be output to a supplier of the classified data. When an input procedure is started for receiving the classified data via the interface means and storing the classified data in the first storage means, the control means outputs the certificate via the interface means in response to a request to output the certificate received via the interface means and, when the supplier certifies the certificate, the control means receives the classified data from the supplier via the interface means.

Preferably, the certificate includes a public key associated with the data storage device, and the data storage device further includes: private key holding means for holding a private key for decrypting data encrypted by the public key; first decrypting means using the private key for decrypting the data encrypted by the public key; session key generating means for generating a first session key peculiar to the predetermined input/output procedures in the predetermined input/output procedures for performing input/output of the classified data; encrypting means for encrypting data by a second session key generated by the supplier; and second decrypting means for decrypting data encrypted by the first session key. In the input procedure, the session key generating means generates the first session key, the first decrypting means uses the private key to decrypt the second session key encrypted by the public key, the encrypting means encrypts the first session key by the second session key received from the first decrypting means, the second decrypting means uses the first session key to decrypt the classified data encrypted by the first session key, the control means provides to the first decrypting means the second session key encrypted by the public key received from the supplier via the interface means, outputs the first session key encrypted by the second session key for providing the first session key via the interface means to the supplier, provides to the second decrypting means the classified data encrypted by the first session key received from the supplier via the interface means, and stores the classified data as decrypted, at a storage position on the first storage means specified by the address.

Preferably, the procedure specifying information is the first session key for specifying the input procedure, and the control means renews the procedure specifying information every time the first session key is generated by the session key generating means.

Preferably, the data storage device further includes signing means for producing signed data for the log information that can be certified by the second session key received from the first decrypting means, and producing signed log information by affixing the produced signed data to the log information. In a re-input procedure for resuming the input procedure when the input procedure is interrupted, the first decrypting means decrypts the second session key encrypted by the public key newly received from the supplier via the interface means, the signing means produces the signed log information by newly received second session key, after the first status stored in the second storage means is renewed, and the control means provides to the first decrypting means the second session key encrypted by the public key newly received from the supplier via the interface means, renews the first status, and outputs the signed log information produced by the signing means for providing the signed log information via the interface means to the supplier.

Preferably, the classified data includes the identification code peculiar to the classified data, and the control means specifies the classified data by the identification code included in the classified data stored at a storage position on the first storage means specified by the address, when the state of storage of the classified data in the first storage means is determined.

Preferably, the control means stops storage of the classified data in the first storage means when mismatch occurs between the identification code included in the received classified data and the identification code included in the log information.

Preferably, the data storage device further includes certifying means for verifying and certifying correctness of an additional certificate of a receiver to which the classified data stored in the first storage means is to be supplied, the additional certificate being received from the receiver. In an output procedure for outputting the classified data via the interface means, the certifying means verifies the additional certificate received from the receiver, and the control means provides to the certifying means the additional certificate received from the receiver via the interface means and, when the additional certificate is not certified by the certifying means, the control means stops the output procedure.

Preferably, the data storage device further includes: certifying means for verifying and certifying correctness of an additional certificate of a receiver to which the classified data stored in the first storage means is to be supplied, the additional certificate being received from the receiver; and additional encrypting means for encrypting data by a public key associated with the receiver that is included in the additional certificate. In an output procedure for outputting the classified data via the interface means, the certifying means certifies the additional certificate received from the receiver, the session key generating means further generates a third session key, the additional encrypting means uses the public key associated with the receiver to encrypt the third session key, the second decrypting means uses the third session key to further decrypt a fourth session key generated by the receiver that is encrypted by the third session key, the encrypting means uses the fourth session key received from the second decrypting means to further encrypt the classified data, and the control means provides to the certifying means the additional certificate received from the receiver via the interface means and, when the certifying means certifies the additional certificate, the control means provides to the additional encrypting means the public key associated with the receiver that is included in the additional certificate, outputs the third session key encrypted by the public key associated with the receiver for providing the third session key to the receiver via the interface means, provides to the second decrypting means the fourth session key encrypted by the third session key received from the receiver via the interface means, obtains the classified data stored at a storage position on the first storage means specified by the address and provides the obtained classified data to the encrypting means, and outputs the classified data encrypted by the fourth session key for providing the classified data to the receiver via the interface means.

Preferably, the procedure specifying information is the fourth session key specifying the output procedure, and the control means renews the procedure specifying information every time the fourth session key is decrypted that is encrypted with the third session key, by the second decrypting means.

Preferably, the classified data includes the identification code peculiar to the classified data, and the control means stops the output procedure without outputting the classified data when mismatch occurs between the identification code included in the classified data stored at a storage position on the first storage means specified by the address and the identification code included in the log information.

Preferably, the data storage device further includes log certifying means for verifying and certifying correctness of signed log information prepared by affixing signed data for additional log information of a receiver of the classified data to the additional log information, and received from the receiver of the classified data via the interface means. In a re-output procedure for resuming an output procedure when the output procedure for outputting the classified data stored in the first storage means via the interface means is interrupted, the log certifying means verifies correctness of the signed log information received from the receiver of the classified data in the interrupted output procedure, and the control means stops the re-output procedure, when it is determined that the signed log information not correct, or when the correctness of the signed log information is certified and it is determined based on the signed log information and the log information stored in the second storage means of the data storage device that the output procedure is not interrupted.

Preferably, the data storage device further includes log certifying means for verifying and certifying correctness of additional signed log information having a sign given to additional log information of a receiver of the classified data by the fourth session key, as received from the receiver via the interface means. In a re-output procedure for resuming an output procedure when the output procedure for outputting the classified data stored in the first storage means via the interface means is interrupted, the log certifying means verifies correctness of the additional signed log information received from the receiver of the classified data in the interrupted output procedure, and when it is determined that the additional signed log information is not correct or when the correctness of the additional signed log information is certified and it is determined that the output procedure is not interrupted based on the additional signed log information and the log information stored in the second storage means of the data storage device, the control means stops the re-output procedure.

Preferably, the classified data is a decryption key for decrypting and using encrypted content data, and the data storage device further comprises third storage means for storing the encrypted content data:

Preferably, the third storage means is a hard disk.

[Embodiments]

Embodiments of the invention will now be described with reference to the drawings. The same or similar parts or portions bear the same reference numbers in the figures, and description thereof is not repeated.

[First Embodiment]

Fig. 1 is a schematic diagram showing a concept of a whole structure of a data distribution system, in which a data storage device according to the invention obtains encrypted content data and a license for decrypting the encrypted content data.

The following description will be given by way of example on a data distribution system, in which terminal device 10 receives a picture data distributed over a digital broadcasting network, and stores the data in a hard disk 20, which is a data storage device attached to terminal device 10. In this system, terminal device 10 is connected to a bidirectional network 30, and receives a license for decrypting encrypted picture data over network 30 from a license providing device 40 for storing it on hard disk 20. Terminal device 10 reproduces the encrypted picture data by an internal reproducing circuit (not shown) dedicated to such reproduction. However, as will become apparent from the following description, the present invention is not restricted to such a case. The present invention is applicable to distribution of other copyrighted materials, i.e., content data such as image data, music data, educational data, reading or recitation data or book data, or programs, e.g., of games. Likewise, the data storage device is not restricted to the hard disk, and may be applied to another data storage device such as a memory card.

Referring to Fig. 1, terminal device 10 receives the encrypted picture data, which is distributed over the digital broadcasting network, via an antenna 11, and stores it on hard disk 20. This picture data may also be referred to as "content data" hereinafter. License providing device 40, which manages and distributes the license including a content key to be used for decrypting the encrypted content data, performs certification processing by determining whether hard disk 20 attached to terminal device 10, which made access for distribution of the license, has correct certification data or not, i.e., whether hard disk 20 is a correct data storage device having a license managing function or not. Only when hard disk 20 is the correct data storage device, license providing device 40 sends the license encrypted in a predetermined encryption manner, which allows decryption only by hard disk 20, to terminal device 10. When terminal device 10 receives the encrypted license via a modem connected to network 30, terminal device 10 sends the encrypted license to hard disk 20 attached thereto.

For example, hard disk 20 in Fig. 1 is removable from terminal device 10. Hard disk 20 attached to terminal device 10 receives the encrypted license received by terminal device 10, decrypts the license encrypted for protecting a copyright and stores the license on hard disk 20. For reproducing the encrypted content data corresponding to the license, terminal device 10 is supplied with the content key included in the license and the encrypted content data.

A user of terminal device 10 can reproduce the content data, which can be decrypted with the content key in terminal device 10.

According to the above structure, the user of terminal device 10, which received and stored the encrypted content data, can receive the license, and thus can reproduce the content data only when terminal device 10 uses hard disk 20, which has a license management function and includes correct certification data.

In the above data distribution system, the provider of the encrypted content data is a broadcasting server of a digital broadcasting company or the like. However, the provider may be license providing device 40 managing the license of the contents, may be a distribution server, which is connected via a communication network such as the Internet, other than license providing device 40, or may be a copy from another user. Thus, the encrypted content data itself may be issued from any portion, and may be received by any portion. In summary, the copyright of the content data can be protected as long as the license allowing decryption of the encrypted content data is controlled strictly.

According to the embodiment of the invention, when the processing is performed to transmit the license between hard disk 20, terminal device 10 and license providing device 40, the provider of the license required for reproducing the encrypted content data performs the verifying and checking processing on the receiver or destination so as to prevent the output of license to an unauthorized device. Further, a structure of a system will be described that achieves copyright protection of content data by specifying a license for which reprocessing is necessary so that there is no double presence of the license when a failure occurs while license transmission process is performed, and that can recover after the failure is ended of the transmission

Fig. 2 illustrates characteristics of data, information and others used for transmission in the data distribution systems shown in Fig. 1.

Data Dc is the content data, which is the picture data in this embodiment. Data Dc is encrypted into a form allowing decryption with a content key Kc. Encrypted content data E(Kc, Dc) which is encrypted in the manner allowing decryption with content key Kc is distributed in this form to users of terminal devices 10 over the digital broadcasting network.

In the following description, the expression E(X, Y) represents that data Y is encrypted into a form allowing decryption with a decryption key X. Together with data Dc, the network distributes additional information Di, which is plaintext information relating, e.g., to copyright of the content data or server access.

License ID (LID), which is a management code for specifying the distribution of the license and specifying each license, is transmitted between license providing device 40 and hard disk 20 via terminal device 10. The license includes data ID (DID), which is a code for identifying data Dc and content key Kc, and control information AC, which relates to restrictions on handling of the license and reproduction in the data storage device, and more specifically relates to the number of licenses, function restrictions and others determined in accordance with designation by the user side.

In the following description, content key Kc and control information AC as well as IDs (DID and LID) will be collectively referred to as a license LIC. DID is identification information assigned to a pair of data Dc and content key Kc, and thus is identification information for identifying encrypted data E(Kc, Dc). In addition to license LIC, DID is also included in additional information Di, which is always handled together with encrypted data E(Kc, Dc) in a manner allowing reference to it.

Fig. 3 illustrates characteristics of data, information and others for certification, which are used in the data distribution system shown in Fig. 1.

Reproducing circuits arranged in the data storage device such as hard disk 20 as well as terminal device 10 are provided with class public keys KPcmy and KPcpy peculiar to them. Class public keys KPcmy and KPcpy can be decrypted with a class private key Kcmy peculiar to the data storage device and a class private key Kcpy peculiar to the reproducing circuit, respectively. These class public keys and class private keys have values, which depend on the types of the reproducing circuit and the data storage device. These class public keys and class private keys are shared by a unit, which is referred to as a "class". A character "y" represents an identifier for identifying the class. The class depends on a manufacturer, a kind of the product, a production lot and others.

Cmy is employed as a class certificate of the data storage device. Cpy is employed as a class certificate of the reproducing circuit. These class certificates have information depending on the classes of the data storage device and the reproducing circuit.

The data storage device stores its class certificate Cmy in the form of KPcmy//Icmy//E(Ka, H(KPcmy//Icmy)) at the time of shipment. The reproducing circuit stores its class certificate Cpy in the form of KPcpy//Icpy//E(Ka, H(KPcpy//Icpy)) at the time of shipment. Expression of "X//Y" represents coupling between X and Y, and H(X) represents a hash value of data X calculated by the hash function. Master key Ka is a private encryption key used for preparing these class certificates. Master key Ka is shared by the whole data distribution system, and is safely managed and operated by a certification authority. Class information Icmy and Icpy are information data including information related to devices in each class and the class public key.

E(Ka, H(KPcmy//Icmy)) and E(Ka, H(KPcpy//Icpy)) are signed data prepared by affixing electronic signatures to KPcmy//Icmy and KPcpy//Icpy, respectively.

The certification authority is a public organization preparing the signature data, and produces signature data E(Ka, H(KPcmy//Icmy)) and E(Ka, H(KPcpy//Icpy)).

As keys for safely and reliably sending license LIC to the data storage device, the system employs an individual public key KPomz set corresponding to each medium, i.e., each data storage device as well as individual private key Komz allowing decryption of the data encrypted with individual public key KPomz. The character "z" in these expressions is an identifier for individually identifying the data storage device.

Every time the data transmission is performed, the data distribution system uses session keys Ks1x and Ks2x produced by license providing device 40, the data storage device (hard disk 20) and terminal device 10.

Session keys Ks1x and Ks2x are symmetric keys generated for each "session", i.e., the unit of communication between license providing device 40, the data storage device (hard disk 20) and the reproducing circuit of terminal device 10, or the unit of access thereto. The "session" includes "distribution session" for distributing the license from license providing device 40 to the data storage device (hard disk 20), "copy/shift session" for copying or shifting the license between the data storage devices, and "reproduction permission session" for outputting the license from the data storage device (hard disk 20) to the reproducing circuit of terminal device 10.

Session keys Ks1x and Ks2x have values peculiar to each session so that these are managed by license providing device 40, the data storage device (hard disk 20) and the reproducing circuit of terminal device 10. More specifically, when the license is to be transmitted, session key Ks1x is generated for each session by the sender side of the license, and session key Ks2x is generated for each session by the receiver side of the license. The character "x" is an identifier for identifying a series of processing in the session. In each session, these session keys are mutually transmitted between the devices. Each device receives the session key produced by the other device, and performs the encryption with the received session key. Then, the device sends license LIC or a part of license LIC including the content key so that the degree of security in the session can be improved.

Fig. 4 is a schematic block diagram showing a structure of license providing device 40 shown in Fig. 1.

License providing device 40 includes a content database (DB) 402 holding the licenses to be managed, a log database 404 storing all communication records in the distribution session for distributing the license, a data processing portion 410 transmitting data to and from content database 402 and log database 404 via a bus BS1 and effecting predetermined processing on it, and a communication device 450 transmitting the data between terminal device 10 and data processing portion 410 over network 30.

Data processing portion 410 includes a distribution control portion 412 for controlling the operation of data processing portion 410 in accordance with the data on bus BS1, a session key generating portion 414 for generating session key Ks1x in the distribution session under control of distribution control portion 412, a KPa holding portion 416 holding certification key KPa of hard disk 20 for decrypting signature data E(Ka, H(KPcmy//Icmy))included in class certificate Cmy of hard disk 20 as sent from terminal device 10, and a certifying portion 418, which receives class certificate Cmy sent from hard disk 20 via communication device 450 and bus BS1, performs decryption processing with certification key KPa received from KPa holding portion 416, performs decryption of signature data E(Ka, H(KPcmy//Icmy)) included in class certificate Cmy and calculation of the hash value of KPcmy//Icmy included in class certificate Cmy, and verifies class certificate Cmy by comparing and checking the results of the above decryption processing and calculation. Data processing portion 410 further includes an encryption processing portion 420 encrypting session key Ks1x produced by session key generating portion 414 with class public key KPcmy extracted from class certificate Cmy by certifying portion, for each distribution session, and then outputting it to bus BS1, and a decryption processing portion 422 decrypting the data encrypted with session key Ks1x and sent from bus BS1, for performing decryption.

Data processing portion 410 further includes an encryption processing portion 424, which encrypts license LIC applied from distribution control portion 412 with individual public key KPomz which is specific for each the data storage device, as applied from decryption processing portion 422, and an encryption processing portion 426, which further encrypts the output of encryption processing portion 424 with session key Ks2x applied from decryption processing portion 422, for outputting it to bus BS1.

Further, individual public key KPomz and session key Ks2x are provided from terminal device 10 after being encrypted with session key Ks1x. Decryption processing portion 422 decrypts them to obtain individual public key KPomz.

Operation of license providing device 40 in distribution session will be described in detail hereinlater using a flowchart.

Fig. 5 is a schematic block diagram showing a structure of terminal device 10 shown in Fig. 1.

Terminal device 10 includes an antenna 102 receiving a signal sent over the digital broadcasting network, a receiving portion 104, which operates to receive the signal from antenna 102 and convert it into a baseband signal, or operates to modulate data to be sent from antenna 102 and apply it to antenna 102, a modem 106 connecting terminal device 10 to network 30, a bus BS2 transmitting data between various portions in terminal device 10, a controller 108 controlling an operation of terminal device 10 via bus BS2, and a hard disk interface portion 110 controlling transmission of data between hard disk 20 and bus BS2.

Terminal device 10 further includes a certification data holding portion 1502 holding class certificate Cpy already described. It is assumed that class y of terminal device 10 is equal to three (y = 3).

Terminal device 10 further includes a Kcp holding portion 1504 holding a class private key Kcp3, which is a decryption key peculiar to the class, and a decryption processing portion 1506 performing decryption on data received from bus BS2 with class private key Kcp3 to obtain session key Ks1x generated by hard disk 20.

Terminal device further includes a session key generating portion 1508, which generates a session key Ks2x, e.g., based on a random number in the reproduction permission session in which content data stored in hard disk 20 is reproduced, for decrypting data communicated with hard disk 20, an encryption processing portion 1510 encrypting, when receiving content key Kc from hard disk 20, session key Ks2x generated by session key generating portion 1508 with session key Ks1 obtained by decryption processing portion 1506 and outputting it to bus BS2, a decryption processing portion 1512 decrypting data on bus BS2 with session key Ks2x and outputting content key Kc, a decryption processing portion 1514, which receives encrypted content data E(Kc, Dc) from bus BS2, and decrypts it with content key Kc sent from decryption processing portion 1512 to provide data Dc to a reproducing portion 1516, reproducing portion 1516 receiving output from decryption processing portion for reproducing content, a D/A converter 1518 converting the output of reproducing portion 1516 from digital signals to analog signals, and a terminal 1520 for providing the output of D/A converter 1518 to an external output device (not shown) such a display monitor.

In Fig. 5, the region enclosed by the dotted line forms reproducing circuit 150 which is a dedicated circuit reproducing picture data by decrypting encrypted content data. For improving security, reproducing circuit 150 is preferably formed of a semiconductor device of one-chip structure. Further, it is preferable that reproducing circuit 150 is formed of an anti-tamper module, which effectively prevents analysis, which may be executed externally.

Operations in the respective sessions of various components of terminal device 10 will be described later in detail with reference to flowcharts.

Fig. 6 is a schematic block diagram showing a structure of hard disk 20 shown in Fig. 1.

As already described, class public key KPcmy and class private key Kcmy are employed for the hard disk, and class certificate Cmy is also employed for the hard disk. In hard disk 20, it is assumed that the natural number y is equal to 1 (y = 1). The natural number z identifying hard disk 20 is equal to 2 (z = 2).

Therefore, hard disk 20 includes a certification data holding portion 202, which holds certification data KPcm1//Icm1//E(Ka, H(KPcm1//Icm1)) as class certificate Cm1, a Kcm holding portion 204 holding class private key Kcm1, a Kom holding portion 206 holding individual private key Kom2, and a KPom holding portion 208 holding individual public key KPom2 allowing decryption with individual private key Kom2.

As described above, owing to provision of the encryption key of the data storage device, i.e., the hard disk drive, the distributed content data and the encrypted content key for each hard disk drive can be managed independently of those for the other hard disk drive, as will be described below.

Hard disk 20 further includes an ATA (AT-Attachment) interface portion 212 communicating signals with HD interface portion 110 of terminal device 10 via terminal 210, bus BS3 that is a data transmission path of hard disk 20, and a decryption processing portion 216 decrypting data which is output from ATA interface portion 212 via controller 214 to bus BS3, with individual private key Kom2 provided from Kon holding portion 206, and outputting license LIC distributed from license providing device 40 to secure data storage unit 250, a certifying portion 220, which receives certification key KPa from a KPa holding portion 218, and decrypts the data provided onto bus BS3 with certification key KPa to provide a result of the decryption to controller 214, and provide the obtained class public key KPcm1 to, and an encryption processing portion 224 encrypting the data, which is selectively applied via a selector switch 262, with session key Ks1x or Ks2x applied selectively by a selector switch 260, and providing it onto bus BS3.

Hard disk 20 further includes a session key generating portion 226 generating session keys Ks1x and Ks2x in each of the distribution, copy/shift and reproduction permission sessions, an encryption processing portion 222 encrypting session key Ks1x output by session key generating portion 226 with class public key KPcpy or KPcmy of reproducing circuit 150 of terminal device 10 obtained by certifying portion 220, and decryption processing portion 228 receiving the data, which is encrypted with session key Ks2x obtained from session key generating portion 226, and decrypting it with session key Ks1x or Ks2x obtained by session key generating portion 226.

Hard disk 20 further includes a decryption processing portion 230 for decrypting data on bus BS3 with class private key Kcm1 which is one of a pair of it and class public key KPcml, and an encryption processing portion 232, which encrypts license LIC with individual public key KPomz (z ≠ 2) received from a hard disk 21 in the destination when license LIC is to be shifted or copied from hard disk 20 to hard disk 21.

Hard disk 20 further includes secure data storage portion 250 storing license LIC for reproducing encrypted content data E (Kc, DC), receiving from bus BS3 the log which is a processing record of the session operated by hard disk 20. License LIC is stored in a license memory 250A of secure data storage portion 250, and the log is stored in a log memory 250B of secure data storage portion 250. Secure data storage portion 250 is a storage region, which is formed of, e.g., a semiconductor memory.

Fig. 7 shows a memory structure in secure data storage portion 250.

Referring to Fig. 7, secure data memory 250A can store a plurality of licenses LIC (content key Kc, control information AC, license ID (LID) and data ID (DID)) corresponding to the fact that hard disk 20 can store a plurality of content data.

In hard disk 20, licenses LIC stored in secure data memory 250A are managed according to storage addresses in secure data storage portion 250. This storage address will be referred to as a "LBA" or "logical block address", hereinafter. All licenses LIC stored or output in each session are specified by the LBA.

Secure data storage portion 250 is provided with validity flag memories 250C. Validity flag memories 250C are provided corresponding to logical block addresses specifying the storage positions on secure data memory 250A, and store flags representing validity/invalidity of the licenses stored at the positions specified by the corresponding logical block addresses, respectively.

When the flag in validity flag memory 250C is "valid", license LIC stored in the storage position on secure data memory 250A specified by the logical block address corresponding to the flag can be used so that the user can reproduce the content data corresponding to this license LIC, or can perform the shift or copy of this license LIC.

When the flag in validity flag memory 250C is "invalid", license LIC stored in the storage position on secure data memory 250A specified by the logical block address corresponding to the flag cannot be used so that controller 214 of hard disk 20 rejects license LIC specified by this logical block address. This state is equivalent to that, in which license LIC is erased. Therefore, the user cannot reproduce the content data corresponding to license LIC. The flag in this validity flag memory 250C becomes valid when the license is newly stored, and becomes invalid when the license is shifted.

Log memory 250B includes a license ID region 2501 storing license ID (LID), which specifies license LIC to be handled in the session, a Ks2x region 2502 storing session key Ks2x, which is produced by the data storage device on the receiver side of license LIC in the session, an ST1 region 2503 storing a status ST1 representing a status of processing in the current session, an ST2 region 2504 storing a status ST2, which represents a storage state of the license corresponding to the license ID stored in license ID region 2501, a KPcmx region 2505, in which the data storage device on the sender side stores class public key KPcmx of the data storage device on the receiver side when outputting the license for the shift/copy, and an LBA region 2506 storing the logical block address indicated for outputting or storing license LIC in the session. In accordance with progression of a series of sessions, the data in the respective regions described above are renewed or referred to. Status ST1 represents one of four statuses of "waiting for reception", "received", "waiting for sending" and "sent", and status ST2 represents one of three statuses of "data present", "no data" and "shifted".

When the session is interrupted due to an unexpected failure occurred during the session, a storage state of license LIC, which is being transmitted in the interrupted session, is determined based on the license ID stored in LID region 2501 of log memory 250B as well as logical block address stored in LBA region 2506, and status ST2 is renewed according to a result of this determination. The sender side of the license in the interrupted session receives license LIC, session key Ks2x and statuses ST1 and ST2, which are stored in log memory 250B on the license receiver side, and checks the contents of the log recorded on the sender side and the received license LIC, session key Ks2x and statuses ST1 and ST2. Thereby, it is determined whether retransmission of the license is allowed or not.

Session key Ks2x is stored for specifying each session, and the fact that session key Ks2x is shared represents that the designation of the license to be transmitted and the processing thereof are shared.

With this configuration, when in particular a considerable number of licenses re stored in secure data memory 250A and it is necessary to specify a license in secure data memory 250 in the case for example a certain cession is interrupted (or necessary to specify whether license is present or not), the storage state of the license can be confirmed easily and status ST2 can be updated.

When the determination is performed for the retransmission, the receiver side of the license provides license ID (LID), session key Ks2x and statuses ST1 and ST2, which are stored in log memory 250B, to the sender side of the license, and these license ID (LID), session key Ks2x and statuses ST1 and ST2 will be collectively referred to as an output log. Class public key KPcmx and the logical block address on the receiver side, which are stored in log memory 250B and are referred to only in hard disk 20, will be collectively referred to as an internal log.

When the output log is output, a storage state of the license in license memory 250A is stored in status ST2 based on license ID (LID) stored in log memory 250B as well as the logical block address thereof, whereby the output log is materialized.

Details will be described later with reference to flowcharts illustrating the respective sessions.

Referring again to Fig. 6, the data storage portion of hard disk 20 will be described. Hard disk 20 further includes normal data storage unit 270 storing encrypted content data. Normal data storage portion 270 includes a disk-like magnetic record medium 2701 storing the data, an electric motor 2702 rotating magnetic record medium 2701, a servo-controller 2703 controlling motor 2702, a seek control portion 2704 controlling a position of a magnetic head on magnetic record medium 2701, and a record/reproduction processing portion 2705 instructing a magnetic head to record or reproduce the data. Normal data storage portion 270 has substantially the same structure as that of a known hard disk, and will not be described in detail.

Hard disk 20 further includes controller 214 for controlling the operations in hard disk 20 such as external transmission of the data via ATA interface portion 212, determination relating to the output of license based on control information AC and management of secure data storage portion 250.

Other components except for normal data storage portion 270, ATA interface portion 212 and terminal 210 are formed in anti-tamper module region.

Operations in the respective sessions of the data distribution system shown in Fig. 1 will now be described.

[Distribution]

First, description will be given on the operation of distributing the license from license providing device 40 to hard disk 20 attached to terminal device 10 in the data distribution system shown in Fig. 1.

Figs. 8 and 9 are first and second flowcharts illustrating processing (distribution session) of the data distribution system shown in Fig. 1, respectively. More specifically, these flowcharts illustrate the processing, in which a user of terminal device 10 requests, via user's terminal device 10, the license distribution of the encrypted content data, and thereby license providing device 40 distributes the license to hard disk 20 attached to terminal device 10.

Before start of the processing in Fig. 8, the user of terminal device 10 connects terminal device 10 to network 30 via modem 106, and thereby connects terminal device 10 to license providing device 40 via network 30. The following description is based on the premise that the above operations are already performed.

Referring to Fig. 8, when the user of terminal device 10 requests the distribution of the license of intended content data, controller 108 of terminal device 10 provides an output request for the class certificate to hard disk 20 via hard disk interface portion 110 (step S1). When controller 214 of hard disk 20 accepts the output request for the class certificate via terminal 210 and ATA interface portion 212 (step S2), it reads class certificate Cm1 = KPcm1//Icm1//E(Ka, H(KPcm1//Icm1)) from certification data holding portion 202 via bus BS3, and provides class certificate Cm1 to terminal device 10 via ATA interface portion 212 and terminal 210 (step S3).

When controller 108 of terminal device 10 accepts class certificate Cm1 sent from hard disk 20 via hard disk interface portion 110 and bus BS2 (step S4), it sends class certificate Cm1 thus accepted to license providing device 40 via modem 106 and network 30 (step S5).

When license providing device 40 receives class certificate Cm1 from terminal device 10 (step S6), it verifies whether received class certificate Cm1 is correct or not (step S7). The verifying processing is performed as follows.

When license providing device 40 accepts class certificate Cm1 = KPcm1//Icm1//E(Ka, H(KPcm1//Icm1)), certifying portion 418 decrypts signature data E(Ka, H(KPcm1//Icm1)), which is included in class certificate Cm1 provided from hard disk 20, with certification key KPa. Further, certifying portion 418 calculates the hash value of KPcm1//Icm1 included in class certificate Cm1, and compares it with the value of H(KPcm1//Icm1) decrypted with certification key KPa. When distribution control portion 412 determines, from the result of the decryption by certifying portion 418, that the foregoing decryption was performed and matching with the hash value occurred, certifying portion 418 certifies the certificate.

When class certificate Cm1 is certified in step S7, distribution control portion 412 approves class certificate Cm1, and accepts class public key KPcm1 (step S8). Next processing is then performed in a step S9. When the class certificate is not certified, distribution control portion 412 does not approve class certificate Cm1, and provides an error notification to terminal device 10 without accepting class certificate Cm1 (step S44 in Fig. 9). When terminal device 10 accepts the error notification (step S45 in Fig. 9), the distribution session ends.

As a result of the certification, when it is determined in license providing device 40 that the access is made from the terminal device, which is provided with the hard disk having the correct class certificate, class public key KPcm1 is accepted in step S8, and distribution control portion 412 produces license ID (LID) (step S9), and further produces control information AC (step S10). Session key generating portion 414 generates a session key Ks1a for distribution (step S11). Encryption processing portion 420 encrypts session key Ks1a with class public key KPcm1, which corresponds to hard disk 20 and is obtained by certifying portion 418, and thereby encrypted data E(KPcm1//Ks1a) is produced (step S12).

Distribution control portion 412 handles license ID (LID) and encrypted session key Ks1a as one data series LID//E(KPcm1//Ks1a), and externally provides it via bus BS1 and communication device 450 (step S13).

When terminal device 10 receives LID//E(KPcm1//Ks1a) over network 30 (step S14), it provides received LID//E(KPcm1//Ks1a) to hard disk 20 (step S15). Controller 214 of hard disk 20 accepts LID//E(KPcm1//Ks1a) via terminal 210 and ATA interface portion 212 (step S16). Controller 214 provides accepted E(KPcm1//Ks1a) to decryption processing portion 230 via BS1. Decryption processing portion 230 performs the decryption processing with class private key Kcm1 peculiar to hard disk 20 held in Kcm holding portion 204 to obtain session key Ks1a, and accepts session key Ks1a (step S17).

When controller 214 of hard disk 20 confirms the acceptance of session key Ks1a produced by license providing device 40, it notifies terminal device 10 of this acceptance via ATA interface portion 212 and terminal 210. When controller 108 of terminal device 10 accepts, via hard disk interface portion 110 and bus BS2, the notification that hard disk 20 accepted session key Ks1a, it provides a notification, which requests production of the session key to be produced in the distribution by hard disk 20, to hard disk 20 via bus BS2 and hard disk interface portion 110 (step S18). When controller 214 of hard disk 20 accepts the notification of request for session key production via terminal 210 and ATA controller 212, controller 214 instructs session key generating portion 226 to generate a session key Ks2a to be produced in the distribution operation by hard disk 20. Session key generating portion 226 generates session key Ks2a (step S19).

Session key generating portion 226 provides session key Ks2a generated thereby to controller 214 via bus BS3, and controller 214 receiving session key Ks2a stores session key Ks2a and license ID (LID) accepted in step S16 in log memory 250B of secure data storage portion 250, and sets status ST1 to "waiting for reception" (step S20).

Subsequently, encryption processing portion 224 encrypts one data series formed of session key Ks2a and individual public key KPom2, which are applied by successively selecting contacts Pd and Pf of selector switch 262, with session key Ks1a applied from decryption processing portion 230 via contact Pb of selector switch 260, and thereby produces E(Ks1a, Ks2a//KPom2) (step S21). Encryption processing portion 224 provides E(Ks1a, Ks2a//KPom2) onto bus BS3. Controller 214 accepts encrypted data E(Ks1a, Ks2a//KPom2) provided onto bus BS3, and provides data

LID//E(Ks1a, Ks2a//KPom2), which is one data series formed of the accepted data and license ID (LID), to terminal device 10 via ATA interface portion 212 and terminal 210 (step S22).

When terminal device 10 accepts data LID//E(Ks1a, Ks2a//KPom2) from hard disk 20 (step S23), it provides the accepted data to license providing device 40 over network 30 (step S24).

When license providing device 40 receives data LID//E(Ks1a, Ks2a//KPom2) (step S25), decryption processing portion 422 executes the processing with session key Ks1a, and accepts session key Ks2a produced by hard disk 20 and individual public key KPom2 of hard disk 20 (step S26).

Distribution control portion 412 obtains data ID (DID) and content key Kc corresponding to license ID (LID) from content database 402 (step S27), and produces license LIC = Kc//AC//DID//LID, which is one data series formed of data ID (LID) and content key Kc thus obtained as well as license ID (LID) and control information AC.

Distribution control portion 412 provides license LIC thus produced to encryption processing portion 424. Encryption processing portion 424 encrypts license LIC with individual public key KPom2 if hard disk 20 obtained by decryption processing portion 422, and thereby produces encrypted data E(KPom2, LIC) (step S28). Encryption processing portion 426 encrypts encrypted data E(KPom2, LIC) received from encryption processing portion 424 with session key Ks2a received from decryption processing portion 422 to produce encrypted data E(Ks2a, E(KPom2, LIC)) (step S29).

Referring to Fig. 9, distribution control portion 412 externally provides encrypted data E(Ks2a, E(KPom2, LIC)) via bus BS1 and communication device 450 (step S30). When terminal device 10 accepts encrypted data E(Ks2a, E(KPom2, LIC)) over network 30 (step S31), it provides the encrypted data thus accepted to hard disk 20 (step S32).

Controller 214 of hard disk 20 accepts encrypted data E(Ks2a, E(KPom2, LIC)) via terminal 210 and ATA interface portion 212 (step S33), and provides it onto bus

BS3. Decryption processing portion 228 decrypts data E(Ks2a, E(KPom2, LIC)) provided onto bus BS3 with session key Ks2a provided from session key generating portion 226, and hard disk 20 accepts encrypted license E(KPom2, LIC) prepared by encrypting license LIC encrypted with individual public key KPom2 (step S34). Decryption processing portion 228 provides encrypted license E(KPom2, LIC) onto bus BS3.

According to the instruction of controller 214, decryption processing portion 216 decrypts encrypted license E(KPom2, LIC) with individual private key Kom to accept license LIC (step S35)..

When controller 214 of hard disk 20 confirms the acceptance of license LIC, it notifies terminal device 10 of the acceptance via ATA interface portion 212 and terminal 210. When controller 108 of terminal device 10 accepts, via hard disk interface portion 110 and bus BS2, the notification of acceptance of license LIC by hard disk 20, controller 108 provides the logical block address, at which received license LIC is stored in secure data storage portion 250 of hard disk 20, to hard disk 20 via hard disk interface portion 110 (step S36). Controller 214 of hard disk 20 accepts the logical block address of destination of license LIC via terminal 210 and ATA interface portion 212 (step S37), and stores the accepted logical block address in log memory 250B (step S38).

Controller 214 compares license ID (LID) included in accepted license LIC with license LID (LID) accepted in step S16, and determines whether these match with each other or not (step S39). When the matching is confirmed, controller 214 determines that accepted license LIC is correct, and stores accepted license LIC at the logical block address, which is received from terminal device 10, in secure data storage portion 250 (step S40).

When controller 214 stores license LIC at the designated logical block address, it sets the flag corresponding to this logical block address of validity flag memory 250C to "valid" (step S41). Controller 214 further sets status ST1 in log memory 250B to "received" (step S42), and notifies terminal device 10 of the fact that the series of processing in the distribution session ends.

When terminal device 10 accepts the notification of the end of processing provided from hard disk 20, the distribution session in the data distribution system normally ends.

When controller 214 determines in step S39 that the mismatching of LID occurs and accepted license LIC is not correct, it provides an error notification to terminal device 10 (step S43), and terminal device 10 receives the error notification (step S45) so that the processing ends.

In the distribution processing illustrated in Figs. 8 and 9, license providing device 40 records histories of the processing in a manner, which has not been described. In connection with this, as shown in Fig. 4, however, license providing device 40 is provided with log database 404, in which processing histories of various processing in the distribution session are stored. Log database 404 stores, in addition to other information, accounting information related to sending of the license.

In the series of steps for distribution processing illustrated in Figs. 8 and 9, a failure may occur during the processing between steps S25 and S44, and thereby the processing may be interrupted. In this case, rewrite processing may be performed. For example, the interruption may occur due to various reasons such as power-off of terminal device 10 during the processing, a failure on the side of license providing device 40 or a failure in communication between terminal device 10 and license providing device 40. When the interruption of processing may occur during a period from the end of step S22, in which all the contents of the output log except for status ST2 stored in log memory 250B of hard disk 20 are stored, to step S44, hard disk 20 can be supplied with the license by performing the rewrite processing. Since the foregoing processing is configured to perform the rewrite processing according to the determination of terminal device 10, the rewrite processing is to be performed when the interruption occurred during the processing from step S25 to step S44 except for the processing in from step S22 to step S24, during which terminal device 10 can determine the progress of processing. When the interruption occurs in the steps other than the above, it is determined that license providing device 40 has not provided the license, and the processing starting from the initial step is performed in accordance with the flowcharts of Figs. 8 and 9.

Likewise, the processing performed in license providing device 40 from step S25 to step S30, before which license providing device 40 outputs the license, is not handled as the target case of the rewrite processing if it is possible to specify the step, in which the interruption of processing occurred, and thereby is handled as the case, in which the processing starting from the initial step is to be performed in accordance with the flowcharts of Figs. 8 and 9.

Figs. 10 to 12 are first to third flowcharts illustrating the rewrite processing performed when a failure occurred during the processing from step S25 to step S44 in the distribution processing illustrated in Figs. 8 and 9.

Referring to Fig. 10, when terminal device 10 determines that a failure occurred during the processing from step S25 to step S44, it provides a request for rewriting of license LIC to license providing device 40 over network 30 (step S101). When distribution control portion 412 accepts the rewrite request via communication device 450 and bus BS1 (step S102), it instructs session key generating portion 414 to produce the session key. Session key generating portion 414 receiving the instruction produces a session key Ks1b for the rewrite processing (step S103). Distribution control portion 412 obtains class public key KPcm1 corresponding to hard disk 20 from log database 402 storing the log of transmission to and from hard disk 20 in this session (step S104), and provides it to encryption processing portion 420. Encryption processing portion 420 receiving class public key KPcm1 encrypts class public key KPcm1 with session key Ks1b to produce E(KPcm1, Ks1b) (step S105). Distribution control portion 412 externally provides E(KPcm1, Ks1b) via bus BS1 and communication device 450 (step S106).

When terminal device 10 accepts E(KPcm1, Ks1b) over network 30 (step S107), it provides accepted E(KPcm1, Ks1b) to hard disk 20 (step S108). Controller 214 of hard disk 20 accepts E(KPcm1, Ks1b) via terminal 210 and ATA interface portion 212 (step S109). Controller 214 provides accepted E(KPcm1, Ks1b) to decryption processing portion 230 via bus BS3. Decryption processing portion 230 decrypts it with class private key Kcm1, which is held by Kcm holding portion 204 and is peculiar to hard disk 20, to provide session key Ks1b so that session key Ks1b is accepted (step S110).

When controller 214 of hard disk 20 confirms the acceptance of session key Ks1b produced by license providing device 40, it provides a notification of the acceptance to terminal device 10 via ATA interface portion 212 and terminal 210. When controller 108 of terminal device 10 accepts, via hard disk interface portion 110 and bus BS2, the notification that hard disk 20 accepted session key Ks1b, it provides an output request for log memory 250B stored in secure data storage portion 250 to hard disk 20 via hard disk interface portion 110 (step S111).

When controller 214 of hard disk 20 accepts the notification of output request of log memory 250B via terminal 210 and ATA controller 212 (step S112), it determines whether license ID (LID) of license LIC stored at the logical block address stored in log memory 250B matches with license ID (LID) stored in log memory 250B or not (step S113).

When controller 214 determines that both license IDs (LID) match with each other, the distribution processing is performed until license LIC is received from license providing device 40, and it is recognized that hard disk 20 has accepted license LIC. Thereby, controller 214 checks the flag stored in validity flag memory 250C corresponding to the license, which is stored at the address designated by the logical block address stored in log memory 250B, and determines the validity of the license (step S114).

When controller 214 determines that the license is valid, it changes status ST2 in log memory 250B to "data present", and then perform the next processing (step S118). When controller 214 determines in step S114 that the license is invalid, it changes status ST2 in log memory 250B to "shifted", and then performs the new processing in step S118.

In step S113, when controller 214 determines that compared license IDs (LID) do not match with each other, it changes status ST2 in log memory 250B to "no data" (step S117).

In this manner, the logical block address stored in log memory 250B is used, and license ID (LID) of license LIC stored at this logical block address can be directly determined based on the logical block address. Thereby, even when license memory 250A has stored a large number of licenses, it is possible to determine presence/absence of the specific license ID (LIC) without retrieving these licenses one by one.

When the processing is performed to change status ST2, controller 214 obtains license ID (LID), statuses ST1 and ST2, and a session key Ks2c from log memory 250B (step S118). In this case, session key Ks2a is stored in log memory 250B, but session key Ks2c obtained from log memory 250B is illustrated for the sake of description. Controller 214 provides session key Ks2c thus obtained to encryption processing portion 224 via bus BS3.

Encryption processing portion 224 encrypts session key Ks2c obtained from bus BS3 with session key Ks1b, which is applied from decryption processing portion 230 via contact Pb of selector switch 260, and produces E(Ks1b, Ks2c) (step S119). Encryption processing portion 224 provides E(Ks1b, Ks2c) thus produced onto bus BS3. Controller 214 accepts E(Ks1b, Ks2c) on bus BS3, produces one data series LID//E(Ks1b, Ks2c)//ST1//ST2 from E(Ks1b, Ks2c) and the data obtained in step S118, and produces hash value H(LID//E(Ks1b, Ks2c)//ST1//ST2) by using the hash function (step S120). Controller 214 provides hash value H(LID//E(Ks1b, Ks2c)//ST1//ST2) to encryption processing portion 224 via bus BS3.

Encryption processing portion 224 encrypts hash value H(LID//E(Ks1b, Ks2c)//ST1//ST2) obtained from bus BS3 with session key Ks1b, which is applied from decryption processing portion 230 via contact Pb of selector switch 260, to produce E(Ks1b, H(LID//E(Ks1b, Ks2c)//ST1//ST2)) (step S121). Encryption processing portion 224 provides E(Ks1b, H(LID//E(Ks1b, Ks2c)//ST1//ST2)) thus produced to bus BS3. Data series LID//E(Ks1b, H(LID//E(Ks1b, Ks2c)//ST1//ST2)) will be referred to as a "receive log", and E(Ks1b, H(LID//E(Ks1b, Ks2c)//ST1//ST2) is signed data prepared by effecting electronic signing on the receive log with session key Ks1b. The purpose of encrypting session key Ks2c stored in log memory 250B with session key Ks1b is to eliminate the possibility of flow-out of the license due to leakage of session key Ks2c.

When controller 214 accepts the signature data sent from bus BS3, it produces signed receive log LID//E(Ks1b, Ks2c)//ST1//ST2//E(Ks1b, H(LID//E(Ks1b, Ks2c)//ST1//ST2)) using the receive log obtained in step S118, and provides it to terminal device 10 via ATA interface portion 212 and terminal 210 (step S122).

When terminal device 10 accepts signed receive log LID//E(Ks1b, Ks2c)//ST1//ST2//E(Ks1b, H(LID//E(Ks1b, Ks2c)//ST1//ST2)) sent from hard disk 20 (step S123), it provides the accepted data to license providing device 40 over network 30 (step S124). License providing device 40 receives signed receive log LID//E(Ks1b, Ks2c)//ST1//ST2//E(Ks1b, H(LID//E(Ks1b, Ks2c)//ST1//ST2)) over network 30 (step S125).

Referring to Fig. 11, license providing device 40 verifies signed receive log LID//E(Ks1b, Ks2c)//ST1//ST2//E(Ks1b, H(LID//E(Ks1b, Ks2c)//ST1//ST2)) thus received (step S126). The verifying processing is performed as follows.

When distribution control portion 412 accepts the signed receive log, it provides the second half of the signed receive log, i.e., signature data E(Ks1b, H(LID//E(Ks1b, Ks2c)//ST1//ST2) to decryption processing portion 422, and instructs session key generating portion 414 to generate session key Ks1b. Decryption processing portion 422 decrypts signature data E(Ks1b, H(LID//E(Ks1b, Ks2c)//ST1//ST2) with session key Ks1b. Distribution control portion 412 calculates the hash value of the first half of the signed receive log, i.e., receive log LID//E(Ks1b, Ks2c)//ST1//ST2, and compares it with the value of H(LID//E(Ks1b, Ks2c)//ST1//ST2) decrypted by decryption processing portion 422. When distribution control portion 412 determines from a result of the decryption by decryption processing portion 422 that the decryption could be performed and the values matched, license providing device 40 certifies that the data series received from hard disk 20 includes the correct data.

When the signed receive log received from hard disk 20 is certified in step S126, distribution control portion 412 searches log database 404 based on accepted license ID (LID) (step S127). When distribution control portion 412 determines that accepted license ID (LID) is stored in log database 404, and is surely the license provided to hard disk 20, it checks the contents of accepted statuses ST1 and ST2 (step S128).

When status ST1 is "waiting for reception", and status ST2 is "no data", distribution control portion 412 determines that hard disk 20 has not accepted license LIC, which was to be sent to hard disk 20, due to a certain failure. Thereby, distribution control portion 412 provides encrypted data E(Ks1b, Ks2c) included in the received data series to decryption processing portion 422, and decryption processing portion 422 decrypts session key Ks2c with session key Ks1b to accept session key Ks2c. Decrypted session key Ks2c is provided to distribution control portion 412 via bus BS1, and is accepted by distribution control portion 412 (step S129)

Distribution control portion 412 compares session key Ks2a, which was being handled when the failure occurred, with the currently accepted session key Ks2c (step S130). When distribution control portion 412 determines that session key Ks2a matches with session key Ks2c, it provides a permission notification for rewriting of license LIC to terminal device 10 (step S133).

In contrast to the above, the data series received from hard disk 20 may not be certified in step S126. Also, in step S127, license ID (LID) received from hard disk 20 may not be stored in log database 404, and thus cannot be determined as the ID of the license provided to hard disk 20. In step S128, it may be determined that license LIC is accepted in hard disk 20. In step S130, it may be determined that session keys Ks2a and Ks2c do not match with each other. In these cases, distribution control portion 412 issues an error notification via bus BS1 and communication device 450 (step S131). When terminal device 10 accepts the error notification over network 30 (step S132), the processing ends. Thus, license providing device 40 rejects the rewriting of the license, and the processing ends.

When controller 108 of terminal device 10 accepts the permission notification, which is issued in step S133 by license providing device 40, in a step S134, it issues a request notification for production of the session key, which is to be produced in the distribution operation by hard disk 20, to hard disk 20 via bus BS2 and hard disk interface portion 110 (step S135).

When hard disk 20 accepts the request notification for production of the session key issued from terminal device 10 based on the rewrite processing permission notification provided from license providing device 40, similar processing is performed except for that session key Ks2b is newly produced and used instead of session key Ks2a in the series of processing from step S19 to the end of the processing illustrated in Figs. 8 and 9. Therefore, a series of processing following step S135 will not be described.

When the interruption occurs in the rewrite processing during the distribution of the license illustrated in the flowcharts of Figs. 10 to 12, processing is performed as follows. When the interruption occurs in any one of steps S101 - S131, S133 and S142 - S160, the rewrite processing can be performed in accordance with the flowcharts of Figs. 10 to 12. When interruption occurs in any one of steps S134 - S141, the license distribution processing illustrated in the flowcharts of Figs. 8 and 9 is restarted from the initial step so that the processing can be resumed.

As described above, it is confirmed that hard disk 20 attached to terminal device 10 holds correct class certificate Cm1. After this confirmation, the encryption keys (session keys), which are produced by license providing device 40 and hard disk 20, respectively, are mutually transmitted with class public key KPcm1, which is sent together with class certificate Cm1 including it. Each side executes the encryption with the received encryption key, and sends the encrypted data to the opposite side so that mutual certification can be practically performed in the processing of transmitting the encrypted data between the opposite sides. Thereby, it is possible to prohibit the unauthorized distribution of the license to the hard disk, and the security of the data distribution system can be improved.

Further, even when the license distribution processing is interrupted, the receive log on hard disk 20, which is the data storage device on the receiver side, is sent to license providing device 40 so that the resending of the license can be performed safely without performing double distribution of the license.

When the logical block address for storing the license on hard disk 20 is instructed, the logical block address is stored as a part of the log. Thereby, when a failure occurs during the distribution session, the state of storage of license LIC, which is to be recorded during the same session, in secure data memory 250A can be directly checked according to the logical block address stored in log memory 250B without searching data in secure data memory 250A capable of storing a large number of license, and the receive log can be produced rapidly. Accordingly, the rewrite processing can be performed rapidly in the distribution processing.

[Shift/Copy]

Fig. 13 is a schematic view showing a concept of a system structure performing copy/shift processing. Referring to Fig. 13, two data storage devices, i.e., two hard disks (HDs) 20 and 21 can be attached to terminal device 10, and it is possible to perform copying and shifting of the license from hard disk 20 to hard disk 21 via terminal device 10.

Since hard disk 21 is a data storage device different from hard disk 20, it holds individual public key KPom5 and individual private key Kom5 different from those of hard disk 20. In this case, identifier z of hard disk 21 is equal to 5 (z = 5), and thus is different from z of hard disk 20 equal to 2. In the following description, the class of hard disk 21 is equal to that of hard disk 20, and thus is equal to one (y = 1). Thus, each of hard disks 20 and 21 holds class certificate Cm1 = KPcm1//Icm1//E(Ka, KPcm1//Icm1) and class private key Kcm1. However, if the class of hard disk 21 is different from one, i.e., the class of hard disk 20, the class certificate and the class private key are different from those of hard disk 21, similarly to the individual public key and individual private key.

Figs. 14 and 15 are first and second flowcharts illustrating the processing (copy/shift session) of the system allowing the copy/shift of the license shown in Fig. 13, respectively. In the illustrated processing, the user of terminal device 10 requests, from terminal device 10, the copy or shift of the license of the encrypted content data so that the license is copied or shifted from hard disk 20 attached to terminal device 10 to hard disk 21 via terminal device 10.

Referring to Fig. 14, when the user of terminal device 10 requests the copy or shift of the license for the intended content data, controller 108 of terminal device 10 issues an output request for the class certificate to hard disk 21 via bus BS2 and hard disk interface portion 110 (step S201). When controller 214 of hard disk 21 accepts the output request for the class certificate via terminal 210 and ATA interface portion 212 (step S202), it reads class certificate Cm1= KPcm1//Icm1//E(Ka, H(KPcm1//Icm1)) from certification data holding portion 202, and provides class certificate Cm1 to terminal device 10 via ATA interface portion 212 and terminal 210 (step S203).

When terminal device 10 receives class certificate Cm1 from hard disk 21 (step S204), it sends received class certificate Cm1 to hard disk 20 (step S205).

When hard disk 20 receives class certificate Cm1 of hard disk 21 from terminal device 10 (step S206), it verifies whether accepted class certificate Cm1 of hard disk 21 is the correct class certificate or not (step S207). The verifying processing is performed as follows.

When hard disk 20 accepts class certificate Cm1 = KPcm1//Icm1//E(Ka, H(KPcm1//Icm1)) of hard disk 21, certifying portion 220 of hard disk 20 decrypts signature data E(Ka, H(KPcm1//Icm1)) included in class certificate Cm1 of hard disk 21 with certification key KPa. Further, certifying portion 220 calculates the hash value of KPcm1//Icm1 included in class certificate Cm1, and compares the hash value with the value of H(KPcm1//Icm1) decrypted by certifying portion 220. When controller 214 of hard disk 20 determines from the result of decryption by certifying portion 220 that the decryption could be performed and the values matched, it determines that accepted class certificate Cm1 of hard disk 21 is the correct certificate.

When it is determined in step S207 that class certificate Cm1 of hard disk 21 is the correct certificate, controller 214 of hard disk 20 approves class certificate Cm1 of hard disk 21, accepts class public key KPcm1 of hard disk 21 included in class certificate Cm1 of hard disk 21, and stores class certificate Cm1 of hard disk 21 in log memory 250B of secure data storage portion 250 of hard disk 20 (step S208). Next processing is then performed in a step S209. When it is not the correct class certificate of hard disk 21, controller 214 issues an error notification to terminal device 10 without approving and accepting class certificate Cm1 of hard disk 21 (step S252 in Fig. 15). When terminal device 10 accepts the error notification (S253 in Fig. 15), the distribution session ends.

When hard disk 20 determines from the result of verification in step S207 that hard disk 21 has the correct class certificate, class certificate Cm1 of hard disk 21 is accepted in step S208 so that session key generating portion 226 in hard disk 20 generates session key Ks1a (step S209). Encryption processing portion 222 encrypts session key Ks1a with class public key KPcm1 of hard disk 21 obtained by certifying portion 220 to produce encrypted data E(KPcm1//Ks1a) (step S210).

Controller 214 provides license ID (LID) and encrypted session key Ks1a as one data series LID//E(KPcm1, Ks1a) to terminal device 10 via ATA interface portion 212 and terminal 210 (step S211).

Controller 214 of hard disk 20 has already obtained license ID (LID) by referring to a management file in advance. The management file is a data file storing management data for managing a relationship between the encrypted content data and the licenses stored on hard disk 20, and is stored in normal data storage portion 270. The contents of the management file are renewed in response to recording or erasing of the encrypted content data as well as writing, shifting and erasing of the license.

When terminal device 10 accepts LID//E(KPcm1//Ks1a) (step S212), it provides accepted LID//E(KPcm1//Ks1a) to hard disk 21 (step S213). Controller 214 of hard disk 21 accepts LID//E(KPcm1//Ks1a) via terminal 210 and ATA interface portion 212 (step S214). Then, controller 214 provides E(KPcm1//Ks1a) to decryption processing portion 230 via bus BS3. Decryption processing portion 230 decrypts it with class private key Kcm1, which is held by Kcm holding portion 204 and is peculiar to hard disk 21, to obtain and accept session key Ks1a (step S215).

When controller 214 of hard disk 21 confirms the acceptance of session key Ks1a produced by hard disk 20, it notifies terminal device 10 of the acceptance via ATA interface portion 212 and terminal 210. When terminal device 10 accepts the notification that hard disk 21 accepted session key Ks1a, terminal device 10 issues to hard disk 21 a notification of production request for the session key to be produced by hard disk 21 in the copy/shift operation (step S216). When controller 214 of hard disk 21 accepts the notification of production request for the session key via terminal 210 and ATA controller 212, it instructs session key generating portion 226 to produce the session key to be produced in the license copy/shift operation. Session key generating portion 226 produces session key Ks2a (step S217).

Session key generating portion 226 provides session key Ks2a produced thereby to controller 214 via bus BS3, and controller 214 receiving session key Ks2a stores license ID (LID) accepted in step S214 and session key Ks2a in log memory 250B of secure data storage portion 250 of hard disk 21, and sets status ST1 to "waiting for reception" (step S218).

Subsequently, encryption processing portion 224 of hard disk 21 encrypts one data series formed of session key Ks2a and individual public key KPom5, which are applied by successively switching selector switch 262 between contacts Pd and Pf, with session key Ks1a applied via contact Pb of selector switch 260 from decryption processing portion 230, and thereby produces E(Ks1a, Ks2a//KPom5) (step S219). Encryption processing portion 224 provides E(Ks1a, Ks2a//KPom5) onto bus BS3. Controller 214 accepts encrypted data E(Ks1a, Ks2a//KPom5) provided onto bus BS3, and provides one series of data LID//E(Ks1a, Ks2a//KPom5), which is formed of the accepted encrypted data and license ID (LID), to terminal device 10 via ATA interface portion 212 and terminal 210 (step S220).

When terminal device 10 accepts LID//E(Ks1a, Ks2a//KPom5) from hard disk 21 (step S221), it outputs the accepted data to hard disk 20 (step S222).

When hard disk 20 accepts data LID//E(Ks1a, Ks2a//KPom5) (step S223), decryption processing portion 228 performs the decryption processing with session key Ks1a to accept session key Ks2a produced by hard disk 21 as well as individual public key KPom5 of hard disk 21 (step S224). Decryption processing portion 228 provides the decrypted session key Ks2a to controller 214 via bus BS3, and controller 214 stores license ID (LID) accepted in step S223 and session key Ks2a in log memory 250B of secure data storage portion 250 of hard disk 20, and sets status ST1 to "waiting for sending" (step S225).

When the processing in step S225 ends, controller 214 of hard disk 20 notifies terminal device 10 of the ending via ATA interface portion 212 and terminal 210. When controller 108 of terminal device 10 accepts the notification sent from hard disk 20 via hard disk interface portion 110 and bus BS2, it provides the logical block address of secure data storage portion 250 of hard disk 20, at which license LIC to be sent from hard disk 20 to hard disk 21 is stored, to hard disk 20 via bus BS2 and hard disk interface portion 110 (step S226). When controller 214 of hard disk 20 accepts the logical block address of destination of license LIC to be sent via terminal 210 and ATA interface portion 212 (step S227), it stores the accepted logical block address in log memory 250B of secure data storage portion 250 (step S228).

Controller 214 determines whether the flag in validity flag memory 250C corresponding to license LIC stored at the accepted logical block address is "valid" or "invalid" (step S229). When the validity flag is "valid", controller 214 obtains the license LIC, which is to be stored at the accepted logical block address, in accordance with the accepted logical block address (step S230).

Referring to Fig. 15, when controller 214 obtains target license LIC, it compares license ID (LID) included in license LIC with license ID (LID) accepted in step S223, and checks whether these IDs match with each other or not (step S231). When controller 214 confirms the matching, it determines control information AC included in obtained license LIC, and checks whether a restriction is imposed on the use or not (step S232).

When controller 214 determines that control information AC does not prohibit the use of license LIC, it applies obtained license LIC to encryption processing portion 232. Encryption processing portion 232 encrypts license LIC with individual public key KPom5 of hard disk 21 obtained by decryption processing portion 228 to produce encrypted data E(KPom5, LIC) (step S233). Encryption processing portion 232 provides encrypted data E(KPom5, LIC) to encryption processing portion 224 via a selector switch Pc, and encryption processing portion 224 encrypts the encrypted data received from encryption processing portion 232 with session key Ks2a received from decryption processing portion 228 to produce encrypted data E(Ks2a, E(KPom5, LIC)) (step S234).

Based on control information AC included in target license LIC, controller 214 then determines whether the sending of license LIC from hard disk 20 to hard disk 21 is "shift" or "copy" (step S235). When controller 214 determines that it is "shift", it sets the flag in validity flag memory 250C corresponding to target license LIC to "invalid" (step S236). When controller 214 determines that it is "copy", the current license may be left on hard disk 20 so that it starts next processing in a step S237 without changing the flag in validity flag memory 250C.

When the processing of validity flag memory 250C ends, controller 214 changes status ST1 in log memory 250B to "sent" (step S237), and sends encrypted data E(Ks2a, E(KPom5, LIC)) to terminal device 10 via ATA interface portion 212 and terminal 210 (step S238).

In some cases, i.e., when the flag in validity flag memory 250C corresponding to the logical block address accepted in step S229 is "invalid", when matching of license ID (LID) does not occur in step S231, or when control information AC included in obtained license LIC prohibits the use of obtained license LIC in step S232, controller 214 issues the error notification to terminal device 10 (step S252). When terminal device 10 accepts the error notification (step S253), the processing ends.

When terminal device 10 accepts encrypted data E(Ks2a, E(KPom5, LIC)) provided from hard disk 20 in step S238 (step S239), it provides the encrypted data thus accepted to hard disk 21 (step S240). When controller 214 of hard disk 21 accepts encrypted data E(Ks2a, E(KPom5, LIC)) via terminal 210 and ATA interface portion 212 (step S241), controller 214 provides it onto bus BS3. Decryption processing portion 228 decrypts data E(Ks2a, E(KPom5, LIC)) provided onto bus BS3 with session key Ks2a provided from session key generating portion 226, and hard disk 21 accepts encrypted license E(KPom5, LIC) prepared by encrypting license LIC with individual public key KPom5 (step S242). Decryption processing portion 228 provides encrypted license E(KPom5, LIC) onto bus BS3.

In accordance with the instruction of controller 214, encrypted license E(KPom5, LIC) is decrypted with individual private key Kom5, and hard disk 21 accepts license LIC (step S243).

When controller 214 confirms the acceptance of license LIC, it notifies terminal device 10 of the acceptance via ATA interface portion 212 and terminal 210. When controller 108 of terminal device 10 receives the notification of acceptance of license

LIC by hard disk 21 via hard disk interface portion 110 and bus BS2, it provides the logical block address, at which received license LIC is to be stored in secure data storage portion 250 of hard disk 21, to hard disk 21 via hard disk interface portion 110 (step S244). When controller 214 of hard disk 21 accepts the logical block address of destination of license LIC via terminal 210 and ATA interface portion 212 (step S245), it stores the accepted logical block address in log memory 250B (step S246).

Controller 214 compares license ID (LID) included in accepted license LIC with license ID (LID) accepted in step S214, and determines whether these IDs match with each other or not (step S247). When these IDs match with each other, controller 214 determines that accepted license LIC is correct, and stores accepted license LIC at the logical block address, which is received from terminal device 10, in secure data storage portion 250 (step S248).

When controller 214 stores license LIC at the designated logical block address, it sets the flag, which corresponds to the logical block address, in validity flag memory 250C to "valid" (step S249). Controller 214 sets status ST1 in log memory 250B to "received" (step S250), and notifies, via ATA interface portion 212 and terminal 210, terminal device 10 of the fact that the series of processing in the copy/shift session ends.

When terminal device 10 accepts the processing end notification sent from hard disk 21, the session of copy/shift between hard disks 20 and 21 normally ends.

When mismatch occurs between the IDs in step S247, controller 214 determines that the accepted license LIC is not correct, and issues the error notification to terminal device 10 via ATA interface portion 212 and terminal 210 (step S251). When terminal device 10 accepts the error notification (step S253), the copy/shift session ends.

Similarly to the distribution session, rewrite processing is to be performed when interruption occurs in the series of processing of the copy/shift session illustrated in Figs. 14 and 15 due to a failure during the processing from step S227 to step S252.

In the copy/shift session illustrated in Figs. 14 and 15, the rewrite processing is to be performed when the interruption occurs during the processing from step S227 to step S235 for the following reasons. The series of processing from step S227 to step S235 is internal processing, and it is impossible to specify the step, in which processing of terminal device 10 failed, among the steps from step S227 to step S238. Therefore, it is assumed that step S236 was executed to invalidate the license in all the cases, and thus the rewrite processing is to be performed as described above.

For the following reasons, the rewrite processing is to be performed for the processing from step S236 to step S247. In the shift processing, the license on hard disk 20 is invalidated in step S236, and will be invalid during the above period from step S236 to step S247. Also, the valid license is not present on hard disk 21 during the above period. Therefore, if the processing is interrupted during the above period, the target license is lost. In the case of copy processing, since the license is not invalidated in step S236, the rewrite processing may be performed similarly to the case of the shift processing, or the copy processing may be restarted from the initial step. In the case of the shift processing, however, only the rewrite processing can restore the license.

The rewrite processing is performed for the processing from step S248 to step S250 for the following reasons. Steps S249 and S250 are performed after the writing of license in step S248, and thus primary processing are already completed before these steps. However, terminal device 10 cannot determine the end of step S248 so that it is assumed that step S248 has not ended, and it is configured to perform the rewrite processing for steps S248 to step S250. When the rewrite processing is performed after the end of step S248, rewriting will be rejected in the rewrite processing.

The rewrite processing is further performed for the processing in step S251 for the following reasons. The processing in step S251 is primarily interrupted only in an extremely special case, but it is impossible to determine the fact that the processing is interrupted in step S251. Therefore, the system is configured to perform the rewrite processing for step S251.

When it is determined in terminal device 10 that the session is the copy of the license as described above, or when it is possible to specify the step, in which the processing is interrupted, among steps S227 - S235 and steps S249 - S251, the rewrite processing is not necessarily required, and it is merely required to execute the copy/shift session illustrated in Figs. 14 and 15 again.

Figs. 16 to 18 are first to third flowcharts, respectively. These flowcharts illustrate the rewrite processing performed when a failure occurred during processing from step S227 to step S252 in the processing flow of the copy/shift session illustrated in Figs. 14 and 15.

Referring to Fig. 16, when terminal device 10 determines that a failure occurred during the processing from step S227 to step S252, it issues a request for resending of license LIC to hard disk 20 (step S301). When controller 214 of hard disk 20 accepts the resending request via terminal 210 and ATA interface portion 212, it determines the state of status ST1 stored in log memory 250B of secure data storage portion 250 (step S302). When controller 214 determines that status ST1 is neither "waiting for sending" nor "sent", i.e., when it is not on the sender side of license LIC in the copy/shift session, the processing moves to a step S371 in Fig. 18.

When status ST1 is "waiting for sending" or "sent", controller 214 of hard disk 20 instructs session key generating portion 226 to produce a session key, and session key generating portion 226 produces session key Ks1a (step S303). When session key Ks1b is produced, controller 214 obtains class public key KPcm1 of hard disk 21, which was accepted before the interruption and has been stored in log memory 250B, in a step S304. Encryption processing portion 222 encrypts session key Ks1b with class public key KPcm1 of hard disk 21 to produce encrypted data E(KPcm1, Ks1b) (step S305). Controller 214 provides encrypted data E(KPcm1, Ks1b) thus produced to terminal device 10 via ATA interface portion 212 and terminal 210 (step S306).

Terminal device 10 accepts encrypted data E(KPcm1, Ks1a) (step S307), and provides it to hard disk 21. Controller 214 of hard disk 21 accepts encrypted data E(KPcm1, Ks1a) via terminal 210 and ATA interface portion 212 (step S309), and provides it to decryption processing portion 230 via bus BS3. Decryption processing portion 230 performs the decryption with class private key Kcm1, which is peculiar to hard disk 21 and is held by Kcm holding portion 204, to obtain and accept session key Ks1a (step S310).

When controller 214 of hard disk 21 confirms the acceptance of session key Ks1b produced by hard disk 20, it notifies terminal device 10 of the acceptance via ATA interface portion 212 and terminal 210. When controller 108 of terminal device 10 accepts the notification sent from hard disk 21 via hard disk interface portion 110 and bus BS2, it issues a request, which requesting output of the log stored in log memory 250B of hard disk 21 to hard disk 20, to hard disk 21 via bus BS2 and hard disk interface portion 110 (step S311). When controller 214 of hard disk 21 accepts the output request for the log via terminal 210 and ATA controller 212 (step S312), it determines whether license ID (LID) of license LIC stored at the logical block address, which is stored in log memory 250B, matches with license ID (LID) stored in log memory 250B or not (step S313).

When these license IDs (LID) match with each other, controller 214 further checks the flag in validity flag memory 250C corresponding to license LIC, which is stored at the logical block address stored in log memory 250B, and determines whether license LIC is valid or invalid (step S314). When the flag in validity flag memory 250C is "valid", controller 214 changes status ST2 in log memory 250B to "data present" (step S315), and next processing starts in a step S318. When the flag in validity flag memory 250C is "invalid", controller 214 changes status ST2 in log memory 250B to "sent" (step S316), and next processing starts in step S318.

When the license IDs (LID) do not match in step S313, controller 214 changes status ST2 in log memory 250B to "no data" (step S317).

In the copy/shift session, as described above, the logical block address stored in log memory 250B is likewise used, and license ID (LID) of the license stored in the storage position of secure data memory 250A designated by the logical block address can be directly confirmed base on the logical block address. Therefore, even when secure data memory 250A has stored a large number of licenses, license ID (LID) can be specified or the presence/absence thereof can be determined without retrieving these licenses one by one.

When status ST2 changes, controller 214 obtains license ID (LID), statuses ST1 and ST2, and session key Ks2c from log memory 250B (step S318). In this case, session key Ks2a is stored in log memory 250B, but session key Ks2c obtained from log memory 250B is illustrated for the sake of description. Controller 214 provides session key Ks2c thus obtained to encryption processing portion 224 via bus BS3.

Encryption processing portion 224 encrypts session key Ks2c with session key Ks1b, which is applied from decryption processing portion 230 via contact Pb of selector switch 260, and produces E(Ks1b, Ks2c) (step S319). Encryption processing portion 224 provides E(Ks1b, Ks2c) thus produced onto bus BS3. Controller 214 accepts E(Ks1b, Ks2c) on bus BS3, produces one receive log LID//E(Ks1b, Ks2c)//ST1//ST2 from E(Ks1b, Ks2c) and the data obtained in step S318, and produces hash value H(LID//E(Ks1b, Ks2c)//ST1//ST2) (step S320). Controller 214 provides hash value H(LID//E(Ks1b, Ks2c)//ST1//ST2) to encryption processing portion 224 via bus BS3.

Encryption processing portion 224 encrypts hash value H(LID//E(Ks1b, Ks2c)//ST1//ST2) obtained from bus BS3 with session key Ks1b, which is applied from decryption processing portion 230 via contact Pb of selector switch 260, to produce signature data E(Ks1b, H(LID//E(Ks1b, Ks2c)//ST1//ST2)) (step S321). Encryption processing portion 224 provides E(Ks1b, H(LID//E(Ks1b, Ks2c)//ST1//ST2)) thus produced to bus BS3.

When controller 214 obtains the signature data from bus BS3, it produces signed receive log LID//E(Ks1b, Ks2c)//ST1//ST2//E(Ks1b, H(LID//E(Ks1b, Ks2c)//ST1//ST2)) using the receive log obtained in step S318, and provides it to terminal device 10 via ATA interface portion 212 and terminal 210 (step S322).

When terminal device 10 accepts signed receive log LID//E(Ks1b, Ks2c)//ST1//ST2//E(Ks1b, H(LID//E(Ks1b, Ks2c)//ST1//ST2)) from hard disk 21 (step S323), it provides the accepted data to hard disk 20 (step S324).

When hard disk 20 accepts signed receive log LID//E(Ks1b, Ks2c)//ST1//ST2//E(Ks1b, H(LID//E(Ks1b, Ks2c)//ST1//ST2)) (step S325), it verifies the accepted data (step S326). The verifying operation is performed as follows.

When controller 214 of hard disk 20 accepts the signed receive log, it provides the second half of the signed receive log, i.e., signature data E(Ks1b, H(LID//E(Ks1b, Ks2c)//ST1//ST2) to decryption processing portion 228, and instructs session key generating portion 226 to generate session key Ks1b. Decryption processing portion 228 decrypts signature data E(Ks1b, H(LID//E(Ks1b, Ks2c)//ST1//ST2) with session key Ks1b. Controller 214 of hard disk 20 calculates the hash value of the first half of the signed receive log, i.e., receive log LID//E(Ks1b, Ks2c)//ST1//ST2, and compares it with the value of H(LID//E(Ks1b, Ks2c)//ST1//ST2) decrypted by decryption processing portion 228. When controller 214 of hard disk 20 determines from a result of the decryption by decryption processing portion 228 that the decryption could be performed and the values matched, controller 214 of hard disk 20 certifies that the data series received from hard disk 21 includes the correct data.

When the signed receive log is verified in step S326, and the data thereof is certified in hard disk 20, controller 214 of hard disk 20 compares license ID (LID) included in the data accepted in step S325 with license ID (LID) stored in log memory 250B (step S327).

When these license IDs (LID) match with each other, controller 214 provides encrypted data E(Ks1b, Ks2c) included in the received data series to decryption processing portion 228, and decryption processing portion 228 decrypts session key Ks2c with session key Ks1b received from session key generating portion 226 to accept session key Ks2c (step S328). Session key Ks2c obtained by the decryption is provided to controller 214 via bus BS3. Then, controller 214 compares session key Ks2a, which was being used when a failure occurred, with currently accepted session key Ks2c, and checks it (step S329). When controller 214 determines that matching occurs between session keys Ks2a and Ks2c, it checks the contents of accepted statuses ST1 and ST2 (step S330).

When received status ST1 is "waiting for reception" and status ST2 is "no data", controller 214 of hard disk 20 determines that license LIC, which was to be sent to hard disk 21, is not accepted by hard disk 21 due to a certain failure. Thereby, controller 214 of hard disk 20 further determines whether license ID (LID) of license LIC, which is stored at the logical block address stored in log memory 250B, matches with license ID (LID) stored in log memory 250B or not (step S331). When these license IDs (LID) match with each other, controller 214 of hard disk 20 checks the flag in validity flag memory 250C corresponding to the logical block address stored in log memory 250B, and determines whether the license LIC is valid or not (step S332). When the flag in validity flag memory 250C is "invalid", controller 214 changes the flag in validity flag memory 250C to "valid" (step S333). When the flag in validity flag memory 250C is "valid", controller 214 starts next processing in a step S334. Controller 214 obtains the logical block address stored in log memory 250B, and provides it to terminal device 10 via ATA interface portion 212 and terminal 210 (step S334).

When controller 108 of terminal device 10 receives the logical block address, at which target license LIC is to be stored, from hard disk 20 via hard disk interface portion 110 and bus BS2 (step S335), controller 108 issues a request notification for production of the session key, which is to be produced on hard disk 21 during the copy/shift operation, to hard disk 21 via bus BS2 and hard disk interface portion 110 (step S336).

When hard disk 21 accepts the production request notification for the session key from terminal device 10, processing is performed similarly to the series of processing from step S217 to the end illustrated in Figs. 14 and 15 except for that session key Ks2b is newly produced and used in stead of session key Ks2a. Therefore, the series of processing following step S336 will not be described.

However, the processing may be ended after step S335 to leave the license on hard disk 20. In this case, the license can be shifted again in accordance with the flowcharts of Figs. 14 and 15.

In connection with the interruption of the rewrite processing during the shifting or writing of the license according to the flowcharts of Figs. 16 - 18, when the processing is interrupted in any one of steps S301 - S344 and steps S347 - S371, the rewrite processing can be performed in accordance with the flowcharts of Figs. 16 - 18 again. When the processing is interrupted in any one of steps S324 - S346, the processing for shifting or copying the license may be performed by starting it from its initial step according to the flowcharts of Figs. 14 and 15, and thereby the processing can be resumed.

In this manner, in connection with the copying of shifting of the license between the plurality of hard disks attached to terminal device 10, processing is performed by determining that class certificate Cm1 received from hard disk 21, i.e., the destination of shifting or copying is valid, and the encryption keys (session keys) are produced by and are transmitted between the respective hard disks, between which the copying or shifting of the licenses are performed with class public key KPcm1 sent together with class certificate Cm1 including it. Each hard disk performs the encryption with the encryption key thus received, and sends the encrypted data to the opposite side. Thereby, it is possible to prohibit the unauthorized copying and shifting of the license to the hard disk. Further, the mutual certification can be practically performed in the processing of transmitting the encrypted data. Thereby, it is possible to protect the license from spoofing of the destination, and the security of the system can be improved.

Further, when the interruption occurs in the copy/shift session for the license, processing is performed similarly to that in the distribution session, and thus is performed as follows. The receive log for license LIC, which is to be handled by the copy/shift session in hard disk 21, i.e., the data storage device on the receiver side, is sent to hard disk 20, i.e., the data storage device on the sender side, and the processing is performed in hard disk 20 to compare the contents stored in log memory 250B of hard disk 20 with license LIC, which is stored in secure data memory 250A and is specified by the logical block address stored in log memory 250B. Further, the flag stored in validity flag memory 250C is referred to. Thereby, in the case where the interrupted copy/shift session is the processing of shifting the license, the rewrite processing can be performed safely without allowing double existence of licenses, which can be used in the two data storage devices, i.e., hard disks 20 and 21.

In addition to the above, when the logical block address for storing the license is designated in hard disk 21, i.e., the data storage device on the receiver side, this logical block address is recorded as a part of the log. Thereby, in the case of occurrence of a failure during the copy/shift session, the state of storage of license LIC, which is to be stored in this session in secure data memory 250A, can be directly checked without searching data in secure data memory 250A capable of storing a large number of licenses. This allows rapid production of the receive log. Accordingly, the rewrite processing can be performed rapidly in the copy/shift processing, similarly to the processing already described. Further, in hard disk 20, i.e., the data storage device on the sender side, it is possible to determine directly the contents and the state (permission/prohibition of use) of license LIC, which is a target of the processing.

As described above, the invention provides the data storage device and the processing manners or procedures, which can perform rapid processing while avoiding the loss of license LIC due to the interruption of the copy/shift session, and also provides the data storage device and the processing manners or procedures, which can achieve safe processing and reliable copyright protection even when the rewrite processing is to be performed.

Processing steps S202, S203, S214, S215, S217 - S220, S241 - S243, S245 - S251, S309, S310, S312 - S322, S337 - S340, S361 - S363 and S365 - S371 of hard disk 21 in Figs. 14 - 18 are the same as processing steps S2, S3, S16, S17, S19 - S22, S33 - S35, S37 - S43, S109, S110, S112 - S122, S136 - S139, S150 - S152 and S154 -

S160 of hard disk 20 in Figs. 8 - 12, respectively. Thus, the processing of hard disk 21 for shifting or copying the license is the same as the processing of hard disk 20 for distributing the license. These kinds of processing are all performed in the data storage devices, i.e., hard disks 20 and 21 as the processing for writing the licenses in the data storage devices.

[Reproduction Permission]

Referring to Fig. 5 again, hard disk 20 serving as the data storage device is attached to terminal device 10 provided with reproducing circuit 150 for reproducing the content data, and hard disk 20 gives the permission of reproduction of the content data to reproducing circuit 150 in terminal device 10.

Fig. 19 is a flowchart illustrating processing (reproduction permission session), in which the user of terminal device 10 issues a reproduction request for the encrypted content data from terminal device 10, and thereby hard disk 20 attached to terminal device 10 gives the permission of reproduction to reproducing circuit 150 in terminal device 10.

Referring to Fig. 19, when the user of terminal device 10 requests the reproduction of the intended content data, controller 108 of terminal device 10 issues an output request for the class certificate to reproducing circuit 150 via bus BS2 (step S401). When certification data holding portion 1502 in reproducing circuit 150 receives the output request for the class certificate from bus BS2 (step S402), it provides class certificate Cp3 = KPcp3//Icp3//E(Ka, H(KPcp3//Icp3)) held thereby onto bus BS2 (step S403).

Controller 108 accepts class certificate Cp3 sent from bus BS2 (step S404), and provides accepted class certificate Cp3 to hard disk 20 via bus BS2 and hard disk interface portion 110 (step S405).

Hard disk 20 accepts class certificate Cp3 sent from terminal device 10 (step S406), and verifies whether accepted class certificate Cp3 is correct or not (step S407). The verifying processing is performed in the same manner as that already described in connection with step S207 in the copy/shift session, and therefore description thereof is not repeated.

When it is determined in step S407 that class certificate Cp3 is correct, controller 214 approves class certificate Cp3, and accepts class public key KPcp3 included in class certificate Cp3 (step S408). Next processing is then performed in a step S409. When class certificate Cp3 is not correct, controller 214 does not approve class certificate Cp3, and issues an error notification to terminal device 10 without accepting class certificate Cp3 (step S435). When terminal device 10 accepts the error notification (step S436), the reproduction permission session ends.

When it is determined, as a result of the verification in step S407, in hard disk 20 that reproducing circuit 150 has the correct class certificate, and class public key KPcp3 is accepted in step S408, session key generating portion 226 of hard disk 20 produces session key Ks1d (step S409). Encryption processing portion 222 encrypts session key Ks1d with accepted class public key KPcp3 to produce encrypted data E(KPcp3, Ks1d) (step S410).

Controller 214 receives encrypted data E(KPcp3, Ks1d) from encryption processing portion 222 via bus BS3, and provides it to terminal device 10 via ATA interface portion 212 and terminal 210 (step S411).

In terminal device 10, controller 108 accepts encrypted data E(KPcp3, Ks1d) via hard disk interface portion 110 and bus BS2 (step S412), and controller 108 provides encrypted data E(KPcp3, Ks1d) thus accepted to reproducing circuit 150 via bus BS2 (step S413). Decryption processing portion 1506 of reproducing circuit 150 accepts encrypted data E(KPcp3, Ks1d) from bus BS2 (step S414), and performs the decryption with class private key Kcp3, which is held by Kcp holding portion 1504 and is peculiar to reproducing circuit 150, to produce and accept session key Ks1d (step S415).

When session key Ks1d is accepted, session key generating portion 1508 produces a session key Ks2d (step S416), and provides session key Ks2d thus produced to encryption processing portion 1510. Encryption processing portion 1510 encrypts session key Ks1d received from decryption processing portion 1506 with session key Ks2d to produce encrypted data E(Ks1d, Ks2d) (step S417). Encryption processing portion 1510 provides encrypted data E(Ks1d, Ks2d) onto bus BS2 (step S418).

Controller 108 accepts encrypted data E(Ks1d, Ks2d) from bus BS2 (step S419), and provides the accepted data to hard disk 20 via bus BS2 and hard disk interface portion 110 (step S420).

Controller 214 of hard disk 20 accepts encrypted data E(Ks1d, Ks2d) via terminal 210 and ATA interface portion 212 (step S421), and provides the accepted data onto bus BS3. Decryption processing portion 228 decrypts encrypted data E(Ks1d, Ks2d) provided onto bus BS3 with session key Ks1d applied from session key generating portion 226, and session key Ks2d is accepted in hard disk 20 (step S422). When session key Ks2d is accepted, controller 214 issues the notification of the acceptance to terminal device 10 via ATA interface portion 212 and terminal 210.

When controller 108 of terminal device 10 receives, via hard disk interface portion 110 and bus BS2, the notification that session key Ks2d is accepted in hard disk 20, it provides the logical block address, at which secure data memory 250A stores target license LIC corresponding to the requested content data, to hard disk 20 via bus BS2 and hard disk interface portion 110.

When controller 214 of hard disk 20 accepts the logical block address of target license LIC via terminal 210 and ATA interface portion 212 (step S424), it determines whether the flag of validity flag memory 250C corresponding to license LIC stored in the accepted logical block address is "valid" or "invalid" (step S425).

When the flag in validity flag memory 250C is "valid", controller 214 obtains target license LIC from license memory 250A based on accepted logical block address (step S426). Controller 214 determines the contents of control information AC included in obtained license LIC (step S427). If control information AC designates the number of allowed times of use, controller 214 increments the number of allowed times of use by one, and next processing is performed in a step S429. If control information

AC does not restrict the times of reproduction, controller 214 provides content key Kc included in obtained license LIC onto bus BS3.

Encryption processing portion 224 encrypts content key Kc, which is provided onto bus BS3, with session key Ks2d received from decryption processing portion 228 to produce encrypted data E(Ks2d, Kc) (step S429), and provides the data thus produced onto bus BS3. Controller 214 provides encrypted data E(Ks2d, Kc) from bus BS3 to terminal device 10 via ATA interface portion 212 and terminal 210 (step S430).

Controller 108 of terminal device 10 accepts encrypted data E(Ks2d, Kc) via hard disk interface portion 110 and bus BS2 (step S431), and provides the accepted data onto bus BS2 (step S432).

When decryption processing portion 1512 of reproducing circuit 150 accepts encrypted data E(Ks2d, Kc) from bus BS2 (step S433), it decrypts encrypted data E(Ks2d, Kc) with session key Ks2d applied from session key generating portion 1508. Thereby, reproducing circuit 150 accepts content key Kc (step S434), and the series of processing of reproduction permission session normally ends.

When the flag of validity flag memory 250C is "invalid" in a step S425, or when contents in control information AC cannot be reproduced in a step S427, controller 214 issues an error notification to terminal device 10 (step S435), and terminal device 10 accepts the error notification (step S436) so that the reproduction permission session ends.

As described above, in connection with the reproduction permission given from the data storage device, i.e., hard disk 20 to reproducing circuit 150 in terminal device 10, content key Kc is likewise sent to reproducing circuit 150 after confirming that reproducing circuit 150 holds correct class certificate Cp3 and that class public key KPcp3 sent together with class certificate Cp3 including it is valid. Thereby, unauthorized reproduction of the content data can be prohibited.

As described above, since the large number of licenses stored in the hard disk are managed in accordance with the logical block addresses, it is possible in the reproduction permission session to obtain directly the license corresponding to the content data requested for reproduction without retrieving it from the large number of data, and thus rapid processing can be achieved.

Although not illustrated in the flowcharts, when reproducing circuit 150 is permitted to reproduce the content, and accepts content key Kc, decryption processing portion 1514 decrypts encrypted data E(Kc, Dc) provided from hard disk 20, and reproducing portion 1516 reproduces data Dc obtained by decryption processing portion 1514 so that D/A converter 1518 performs digital-to-analog conversion to provide reproduction signals to terminal 1520 connected to a monitor or a speaker.

All the description already given relates to the license for the content data. However, the target is not limited to the foregoing license, and may be expanded to general classified data to be handled under confidentiality. This is because the foregoing means and manners can protect the confidentiality of data, and can achieve the object of the invention relating to the specifying of the classified data in the data storage device.

Although the present invention has been described and illustrated in detail, it is clearly understood that the same is by way of illustration and example only and is not to be taken by way of limitation, the spirit and scope of the present invention being limited only by the terms of the appended claims.

[Brief Description of the Drawings]

Fig. 1 is a schematic view showing a concept of a data distribution system.

Fig. 2 illustrates characteristics of data, information and others transmitted in the data distribution systems shown in Fig. 1.

Fig. 3 illustrates characteristics of data, information and others used for certification in the data distribution systems shown in Fig. 1.

Fig. 4 is a schematic block diagram showing a structure of a license providing device shown in Fig. 1.

Fig. 5 is a schematic block diagram showing a structure of a terminal device shown in Fig. 1.

Fig. 6 is a schematic block diagram showing a structure of a hard disk attached to the terminal device shown in Fig. 1.

Fig. 7 shows a memory structure of a secure data storage portion in the hard disk shown in Fig. 6.

Fig. 8 is a first flowchart illustrating distribution processing in the data distribution systems shown in Fig. 1.

Fig. 9 is a second flowchart illustrating the distribution processing in the data distribution systems shown in Fig. 1.

Fig. 10 is a first flowchart illustrating the rewrite processing during the distribution processing in the data distribution system shown in Fig. 1.

Fig. 11 is a second flowchart illustrating the rewrite processing during the distribution processing in the data distribution system shown in Fig. 1.

Fig. 12 is a third flowchart illustrating the rewrite processing during the distribution processing in the data distribution system shown in Fig. 1.

Fig. 13 is a schematic view showing a concept of a system structure performing copy/shift processing.

Fig. 14 is a first flowchart illustrating the copy or shift processing in the system shown in Fig. 13.

Fig. 15 is a second flowchart illustrating the copy or shift processing in the system shown in Fig. 13.

Fig. 16 is a first flowchart illustrating the rewrite processing during the copy or shift processing in the system shown in Fig. 13.

Fig. 17 is a second flowchart illustrating the rewrite processing during the copy or shift processing in the system shown in Fig. 13.

Fig. 18 is a third flowchart illustrating the rewrite processing during the copy or shift processing in the system shown in Fig. 13.

Fig. 19 is a flowchart illustrating reproduction permission processing effected on a terminal device shown in Fig. 5.

[Description of the Reference Characters]

10 terminal device, 11 antenna, 20, 21 hard disk, 30 network, 40 license providing device, 102 antenna, 104 receiving portion, 106 modem, 108 controller, 110 hard disk interface portion, 150 reproducing circuit, 202, 1502 certification data holding portion, 204 Kcm holding portion, 206 Kom holding portion, 208 KPom holding portion, 210,1520 terminal, 212 ATA interface portion, 214 controller, 216, 228, 230, 422, 1506, 1512, 1514 decryption processing portion, 218, 416 KPa holding portion, 220, 418 certifying portion, 222, 224, 232, 420, 424, 426, 1510 encryption processing portion, 226, 414, 1508 session key generating portion, 250 secure data storage portion, 250A secure data memory, 250B log memory, 250C validity flag memory, 260, 262 selector switch, 270 normal data storage portion, 402 content DB, 404 log DB, 410 data processing portion , 412 distribution control portion, 450 communication device, 1504 Kcp holding portion, 1516 reproducing portion, 1518 D/A converter, 2501 license ID region, 2502 Ks2x region, 2503 ST1 region, 2504 ST2 region, 2505 KPcmx region, 2506 LBA region, 2701 magnetic record medium, 2702 motor, 2703 servo control portion, 2704 seek control portion, 2705 record/reproduction processing portion, BS1-BS3 bus

FIG. 1

11 CONTENT DATA

40 LICENSE PROVIDING DEVICE

FIG. 2

SYMBOL	NAME	ATTRIBUTE	CHARACTERISTICS
Dc	DATA	PECULIAR TO DATA	EX.: MOVIE, MUSIC, READING, EDUCATIONAL OR IMAGE DATA, OR GAME PROGRAM RECORDED AND MANAGED AS ENCRYPTED CONTENT DATA E(Kc, Dc) ENCRYPTED WITH Kc
Di	DATA INFORMATION	PECULIAR TO DATA	PLAINTEXT DATA RELATED TO Dc AND INCLUDING DID
DID	DATA ID	PECULIAR TO DATA	MANAGEMENT CODE FOR SPECIFYING Dc AND Kc
Kc	CONTENT KEY	PECULIAR TO DATA	SYMMETRIC KEY ENCRYPTING/DECRYPTING ENCRYPTED DATA
Ac	CONTROL INFORMATION	PECULIAR TO LICENSE	RESTRICTIONS RELATED TO REPRODUCTION AND LICENSE HANDLING
LID	LICENSE ID	PECULIAR TO LICENSE	MANAGEMENT CODE FOR SPECIFYING LICENSE
LIC	LICENSE	PECULIAR TO LICENSE	GENERALLY REPRESENTING Kc//AC//DID//LID

FIG. 3

	SYMBOL	NAME	CHARACTERISTIC
LICENSE PROVIDING DEVICE	KPa	CERTIFICATION KEY	PUBLIC DECRYPTION KEY FOR VERIFYING CERTIFICATE BY CERTIFICATION AUTHORITY OPERATED BY LICENSE PROVIDER SIDE
	Ks1x	SESSION KEY	TEMPORARY KEY PRODUCED FOR EVERY LICENSE DISTRIBUTION SYMMETRIC KEY
DATA STORAGE DEVICE (HARD DISK)	Ka	MASTER KEY	PRIVATE ENCRYPTION KEY USED FOR PREPARING CLASS CERTIFICATES, AND OPERATED BY CERTIFICATION AUTHORITY
	KPa	CERTIFICATION KEY	PUBLIC DECRYPTION KEY FOR VERIFYING CERTIFICATE BY CERTIFICATION AUTHORITY OPERATED BY LICENSE PROVIDER SIDE
	KPcmy	CLASS PUBLIC KEY	ENCRYPTION KEY ASSIGNED TO CLASS (UNIT SUCH AS TYPE) OF DEVICE "y" IS IDENTIFIER IDENTIFYING CLASS
	Kcmy	CLASS PRIVATE KEY	ASYMMETRIC DECRYPTION KEY DECRYPTING DATA ENCRYPTED WITH CLASS PUBLIC KEY KPcmy

	Icmy	CLASS INFORMATION	INFORMATION DATA OF DEVICE AND CLASS PUBLIC KEY IN EACH CLASS
	Cmy	CLASS CERTIFICATE	Cmy = KPcmy//Icmy//E(Ka, H(KPcmy//Icmy)) CORRECTNESS IS VERIFIED WITH CERTIFICATION KEY KPa
	KPomz	INDIVIDUAL PUBLIC KEY	INDIVIDUAL PUBLIC ENCRYPTION KEY HAVING SPECIFIC VALUE FOR EACH DATA STORAGE DEVICE "z" IS IDENTIFIER IDENTIFYING DATA STORAGE DEVICE
	Komz	INDIVIDUAL PRIVATE KEY	ASYMMETRIC DECRYPTION KEY DECRYPTING DATA ENCRYPTED WITH INDIVIDUAL PUBLIC KEY KPomz
	Ks1x	SESSION KEY	TEMPORARY KEY PRODUCED BY LICENSE PROVIDER SIDE FOR EVERY LICENSE TRANSMISSION SYMMETRIC KEY
	Ks2x	SESSION KEY	TEMPORARY KEY PRODUCED BY LICENSE RECEIVER SIDE FOR EVERY LICENSE TRANSMISSION SYMMETRIC KEY
REPRODUCING CIRCUIT	KPcpy	CLASS PUBLIC KEY	ENCRYPTION KEY ASSIGNED TO CLASS (UNIT SUCH AS TYPE) OF DEVICE "y" IS IDENTIFIER IDENTIFYING CLASS
	Kcpy	CLASS PRIVATE KEY	ASYMMETRIC DECRYPTION KEY DECRYPTING DATA ENCRYPTED WITH CLASS PUBLIC KEY KPcpy
	Icpy	CLASS INFORMATION	INFORMATION DATA OF DEVICE AND CLASS PUBLIC KEY IN EACH CLASS
	Cpy	CLASS CERTIFICATE	Cpy = KPcpy//Icpy//E(Ka, H(KPcpy//Icpy)) CORRECTNESS IS VERIFIED WITH CERTIFICATION KEY KPa
	Ks2x	SESSION KEY	TEMPORARY KEY PRODUCED BY LICENSE RECEIVER SIDE FOR EVERY LICENSE TRANSMISSION SYMMETRIC KEY

FIG. 4

①	COMMUNICATION NETWORK
450	COMMUNICATION DEVICE
412	DISTRIBUTION CONTROL
426	ENCRYPTION Ks2
424	ENCRYPTION KPomz
422	DECRYPTION Ks1
420	DECRYPTION KPcmy

414	Ks GENERATION
418	CERTIFICATION
416	CERTIFICATION KEY KPa
402	CONTENT DB
404	LOG DATABASE

FIG. 5

30	NETWORK
104	RECEIVING
106	MODEM
108	CONTROLLER
110	HD INTERFACE
1516	REPRODUCTION
150	REPRODUCING CIRCUIT
1514	DECRYPTION Kc
1512	DECRYPTION Ks2
1502	CLASS CERTIFICATE Cp3
1506	DECRYPTION Kcp3
1510	ENCRYPTION Ks2
!504	Kcp HOLDING Kcp3
1508	Ks2 GENERATION

FIG. 6

214	CONTROLLER
250	SECURE DATA STORAGE PORTION (MEMORY)
2702	MOTOR
2705	RECORD/REPRODUCTION PROCESSING
2704	SEEK CONTROL
2703	SERVO CONTROL

202	CLASS CERTIFICATE HOLDING Cm1
226	Ks GENERATION Ks1x OR Ks2x
220	CERTIFICATION
218	KPa HOLDING
222	ENCRYPTION KPcxy
216	DECRYPTION Kom2
206	Kom HOLDING Kom2

FIG. 7

①	SECURE DATA STORAGE PORTION
②	SECURE DATA MEMORY
③	VALIDITY FLAG MEMORY
④	LOG MEMORY
⑤	OUTPUT LOG
2501	LID REGION
2502	Ks2x REGION
2503, 2504	STATUS REGION
⑥	INTERNAL LOG
2505	KPcmx REGION
2506	LBA REGION

FIG. 8

①	LICENSE PROVIDING DEVICE 40
②	TERMINAL DEVICE 10
③	START
S1	ISSUE OUTPUT REQUEST FOR CERTIFICATE
S2	ACCEPT OUTPUT REQUEST FOR CERTIFICATE
S3	PROVIDE Cm1

S4 ACCEPT Cm1

S5 PROVIDE Cm1

S6 ACCEPT Cm1

S7 VERIFY Cm1

④ UNCERTIFIED

⑤ CERTIFIED

S8 ACCEPT KPcm1

S9 PRODUCE LID

S10 PRODUCE AC

S11 PRODUCE Ks1a

S12 ENCRYPT Ks1a WITH KPcm1 TO PRODUCE E(KPcm1, Ks1a)

S13 PROVIDE LID//E(KPcm1, Ks1a)

S14 ACCEPT LID//E(KPcm1, Ks1a)

S15 PROVIDE LID//E(KPcm1, Ks1a)

S16 ACCEPT LID//E(KPcm1, Ks1a)

S17 DECRYPT LID//E(KPcm1, Ks1a) WITH Kcm1 TO ACCEPT Ks1a

S18 PROVIDE SESSION KEY REQUEST

S19 PRODUCE SESSION KEY Ks2a

S20 STORE LID AND Ks2a IN LOG MEMORY

CHANGE ST1 TO "WAITING FOR RECEPTION"

S21 ENCRYPT Ks2a AND KPom2 WITH Ks1a TO PRODUCE E(Ks1a, Ks2a//KPom2)

S22 PROVIDE LID//E(Ks1a, Ks2a//KPom2)

S23 ACCEPT LID//E(Ks1a, Ks2a//KPom2)

S24 PROVIDE LID//E(Ks1a, Ks2a//KPom2)

⑥ TARGET OF REWRITE PROCESSING

S25 ACCEPT LID//E(Ks1a, Ks2a//KPom2)

S26 DECRYPT E(Ks1a, Ks2a//KPom2) WITH Ks1a TO ACCEPT Ks2a AND KPom2

S27 OBTAIN LID AND Kc FROM CONTENT DB (ESTABLISH LIC)

S28 ENCRYPT LIC WITH KPom2 TO PRODUCE E(KPom2, LIC)

S29 ENCRYPT E(KPom2, LIC) WITH Ks2a TO PRODUCE E(Ks2a, E(KPom2, LIC))

⑦ TO S44

⑧ TO S30

FIG. 9

① LICENSE PROVIDING DEVICE 40

② TERMINAL DEVICE 10

③ FROM S7

④ FROM S29

S30 PROVIDE E(Ks2a, E(KPom2, LIC))

S31 ACCEPT E(Ks2a, E(KPom2, LIC))

S32 PROVIDE E(Ks2a, E(KPom2, LIC))

S33 ACCEPT E(Ks2a, E(KPom2, LIC))

S34 DECRYPT E(Ks2a, E(KPom2, LIC)) WITH Ks2a TO ACCEPT E(KPom2, LIC)

S35 DECRYPT E(KPom2, LIC) WITH Kom2 TO ACCEPT LIC

S36 PROVIDE DESTINATION LBA OF LIC

S37 ACCEPT DESTINATION LBA OF LIC

S38 STORE DESTINATION LBA IN LOG MEMORY

S39 LIDS MATCH

⑤ MATCH

⑥ MISMATCH

S40 STORE LIC AT DESTINATION LBA

S41 CHANGE VALIDITY FLAG FOR DESTINATION LBA TO "VALID"

S42 CHANGE ST1 IN LOG MEMORY TO "RECEIVED"

S43	ISSUE ERROR NOTIFICATION
S45	ACCEPT ERROR NOTIFICATION
⑦	END DUE TO WRITE REJECTION
S44	ISSUE ERROR NOTIFICATION
⑧	TARGET OF REWRITE PROCESSING
⑨	NORMAL END

FIG. 10

①	LICENSE PROVIDING DEVICE 40
②	TERMINAL DEVICE 10
③	START REWRITE PROCESSING
④	TARGET OF REWRITE PROCESSING
S101	PROVIDE REWRITE REQUEST
S102	ACCEPT REWRITE REQUEST
S103	PRODUCE Ks1b
S104	OBTAIN KPcm1 FROM LOG DB
S105	ENCRYPT Ks1b WITH KPcm1 TO PRODUCE E(KPcm1, Ks1b)
S106	PROVIDE E(KPcm1, Ks1b)
S107	ACCEPT E(KPcm1, Ks1b)
S108	PROVIDE E(KPcm1, Ks1b)
S109	ACCEPT E(KPcm1, Ks1b)
S110	DECRYPT E(KPcm1, Ks1b) WITH Kcm1 TO ACCEPT Ks1b
S111	PROVIDE LOG OUTPUT REQUEST
S112	ACCEPT LOG OUTPUT REQUEST
S113	LID OF DATA AT LBA STORED IN LOG MEMORY MATCHES WITH LID STORED IN LOG MEMORY
⑤	MISMATCH
⑥	MATCH

S114 DATA AT LBA STORED IN LOG MEMORY IS VALID?

⑦ VALID

⑧ INVALID

S115 CHANGE ST2 IN LOG MEMORY TO "DATA PRESENT"

S116 CHANGE ST2 IN LOG MEMORY TO "SHIFTED"

S117 CHANGE ST2 IN LOG MEMORY TO "NO DATA"

S118 OBTAIN OUTPUT LOG (LID//Ks2a//ST1//ST2) FROM LOG MEMORY

S119 ENCRYPT Ks2c WITH Ks1b TO PRODUCE E(Ks1b, Ks2c)

S120 PRODUCE H(LID//E(Ks1b, Ks2c)//ST1//ST2)

S121 ENCRYPT H(LID//E(Ks1b, Ks2c)//ST1//ST2) WITH Ks1b TO PRODUCE E(Ks1b, H(LID//E(Ks1b, Ks2c)//ST1//ST2))

S122 PROVIDE LID//E(Ks1b, LID//ST1//ST2//E(Ks1b, H(LID//E(Ks1b, Ks2c)//ST1//ST2))

S123 ACCEPT LID//E(Ks1b, LID//ST1//ST2//E(Ks1b, H(LID//E(Ks1b, Ks2c)//ST1//ST2))

S124 PROVIDE LID//E(Ks1b, LID//ST1//ST2//E(Ks1b, H(LID//E(Ks1b, Ks2c)//ST1//ST2))

S125 ACCEPT LID//E(Ks1b, LID//ST1//ST2//E(Ks1b, H(LID//E(Ks1b, Ks2c)//ST1//ST2))

S126 ⌒ TO S126

FIG. 11

① LICENSE PROVIDING DEVICE 40

② TERMINAL DEVICE 10

③ FROM S125

S126 VERIFY LID//E(Ks1b, LID//ST1//ST2//E(Ks1b, H(LID//E(Ks1b, Ks2c)//ST1//ST2))

④ UNCERTIFIED

⑤ CERTIFIED

S127 SEARCH LOG DB WITH LID

⑥ NO DATA PROVISION

⑦ DATA PROVISION

S128 CHECK ST1, ST2

⑧ ALREADY ACCEPTED

⑨ NOT ACCEPTED

S129 DECRYPT E(Ks1b, Ks2c) WITH Ks1b TO ACCEPT Ks2c

S130 Ks2a: Ks2c

⑩ MISMATCH

⑪ MATCH

S131 ISSUE ERROR NOTIFICATION

⑫ TARGET OF REWRITE PROCESSING

S132 ACCEPT ERROR NOTIFICATION

S133 PROVIDE PERMISSION NOTIFICATION

S134 ACCEPT PERMISSION NOTIFICATION

S135 PROVIDE SESSION KEY REQUEST

S136 PRODUCE SESSION KEY Ks2b

S137 STORE LID AND Ks2b IN LOG MEMORY
CHANGE ST1 TO "WAITING FOR RECEPTION"

S138 ENCRYPT Ks2b AND KPom2 WITH Ks1b TO PRODUCE E(Ks1b, Ks2b//KPom2)

S139 PROVIDE LID//E(Ks1b, Ks2b//KPom2)

S140 ACCEPT LID//E(Ks1b, Ks2b//KPom2)

S141 PROVIDE LID//E(Ks1b, Ks2b//KPom2)

⑬ TARGET OF REWRITE PROCESSING

S142 ACCEPT LID//E(Ks1b, Ks2b//KPom2)

S143 DECRYPT E(Ks1b, Ks2b//KPom2) WITH Ks1b TO ACCEPT Ks2b AND

KPom2
S144 OBTAIN LID AND Kc FROM CONTENT DB (ESTABLISH LIC)
S145 ENCRYPT LIC WITH KPom2 TO PRODUCE E(KPom2, LIC)
S146 ENCRYPT E(KPom2, LIC) WITH Ks2b TO PRODUCE E(Ks2b, E(KPom2, LIC))
⑭ TO S147

FIG. 12
① LICENSE PROVIDING DEVICE 40
② TERMINAL DEVICE 10
③ FROM S146
S147 PROVIDE E(Ks2b, E(KPom2, LIC))
④ TARGET OF REWRITE PROCESSING
S148 ACCEPT E(Ks2b, E(KPom2, LIC))
S149 PROVIDE E(Ks2b, E(KPom2, LIC))
S150 ACCEPT E(Ks2b, E(KPom2, LIC))
S151 DECRYPT E(Ks2b, E(KPom2, LIC)) WITH Ks2b TO ACCEPT E(KPom2, LIC)
S152 DECRYPT E(KPom2, LIC) WITH Kom2 TO ACCEPT LIC
S153 PROVIDE DESTINATION LBA OF LIC
S154 ACCEPT DESTINATION LBA OF LIC
S155 STORE DESTINATION LBA IN LOG MEMORY
S156 LIDS MATCH
⑤ MATCH
⑥ MISMATCH
S157 STORE LIC IN DESTINATION LBA
S158 CHANGE VALIDITY FLAG FOR DESTINATION LBA TO "VALID"
S159 CHANGE ST1 IN LOG MEMORY TO "RECEIVED"

S160	ISSUE ERROR NOTIFICATION
S161	ACCEPT ERROR NOTIFICATION
⑦	END DUE TO WRITE REJECTION
⑧	NORMAL END

FIG. 13

10	TERMINAL DEVICE
①	BUS

FIG. 14

①	TERMINAL DEVICE 10
②	START
S201	ISSUE OUTPUT REQUEST FOR CERTIFICATE
S202	ACCEPT OUTPUT REQUEST FOR CERTIFICATE
S203	PROVIDE Cm1
S204	ACCEPT Cm1
S205	PROVIDE Cm1
S206	ACCEPT Cm1
S207	VERIFY Cm1
③	UNCERTIFIED
④	CERTIFIED
S208	ACCEPT AND STORE KPcm1 IN LOG MEMORY
S209	PRODUCE Ks1a
S210	ENCRYPT Ks1a WITH KPcm1 TO PRODUCE E(KPcm1, Ks1a)
S211	PROVIDE LID//E(KPcm1, Ks1a)
S212	ACCEPT LID//E(KPcm1, Ks1a)
S213	PROVIDE LID//E(KPcm1, Ks1a)
S214	ACCEPT LID//E(KPcm1, Ks1a)

S215 DECRYPT LID//E(KPcm1, Ks1a) WITH Kcm1 TO ACCEPT Ks1a

S216 PROVIDE SESSION KEY REQUEST

S217 PRODUCE SESSION KEY Ks2a

S218 STORE LID AND Ks2a IN LOG MEMORY

CHANGE ST1 TO "WAITING FOR RECEPTION"

S219 ENCRYPT Ks2a AND KPom5 WITH Ks1a TO PRODUCE E(Ks1a, Ks2a//KPom5)

S220 PROVIDE LID//E(Ks1a, Ks2a//KPom5)

S221 ACCEPT LID//E(Ks1a, Ks2a//KPom5)

S222 PROVIDE LID//E(Ks1a, Ks2a//KPom5)

S223 ACCEPT LID//E(Ks1a, Ks2a//KPom5)

S224 DECRYPT E(Ks1a, Ks2a//KPom5) WITH Ks1a TO ACCEPT Ks2a AND KPom5

S225 STORE LID AND Ks2a IN LOG MEMORY

CHANGE ST1 TO "WAITING FOR RECEPTION"

S226 PROVIDE STORAGE LBA OF TARGET LIC

⑤ TARGET OF REWRITE PROCESSING

S227 ACCEPT STORAGE LBA OF TARGET LIC

S228 STORE LBA IN LOG MEMORY

S229 VALIDITY FLAG FOR STORAGE LBA

⑥ INVALID

⑦ VALID

S230 OBTAIN LIC BASED ON LBA

⑧ TO S252

⑨ TO S231

FIG. 15

① TERMINAL DEVICE 10

②	FROM S207, S229
③	FROM S230
S231	LID MATCH
④	MISMATCH
⑤	MATCH
S232	CHECK AC
⑥	PROHIBITED
S233	ENCRYPT LIC WITH KPom5 TO PRODUCE E(KPom5, LIC)
S234	ENCRYPT E(KPom5, LIC) WITH Ks2a TO PRODUCE E(Ks2a, E(KPom5, LIC))
S235	CHECK AC
⑦	COPY
⑧	SHIFT
S236	CHANGE VALIDITY FLAG FOR LBA TO "INVALID"
S237	CHANGE ST1 OF LOG MEMORY TO "SENT"
S238	PROVIDE E(Ks2a, E(KPom5, LIC))
S239	ACCEPT E(Ks2a, E(KPom5, LIC))
S240	PROVIDE E(Ks2a, E(KPom5, LIC))
S241	ACCEPT E(Ks2a, E(KPom5, LIC))
S242	DECRYPT E(Ks2a, E(KPom5, LIC)) WITH Ks2a TO ACCEPT E(KPom5, LIC)
S243	DECRYPT E(KPom5, LIC) WITH Kom5 TO ACCEPT LIC
S244	PROVIDE DESTINATION LBA OF LIC
S245	ACCEPT DESTINATION LBA OF LIC
S246	STORE DESTINATION LBA IN LOG MEMORY
S247	LID MATCH
⑨	MATCH
⑩	MISMATCH

S248	STORE LIC IN DESTINATION LBA
S249	CHANGE VALIDITY FLAG FOR DESTINATION LBA TO "VALID"
S250	CHANGE ST1 IN LOG MEMORY TO "RECEIVED"
S251	ISSUE ERROR NOTIFICATION
S253	ACCEPT ERROR NOTIFICATION
⑪	END DUE TO WRITE REJECTION
⑫	NORMAL END
S252	ISSUE ERROR NOTIFICATION
⑬	TARGET OF REWRITE PROCESSING

FIG. 16

①	TERMINAL DEVICE 10
②	START REWRITE PROCESSING
③	TARGET OF REWRITE PROCESSING
S301	ST1 STORED IN LOG MEMORY?
④	INVALID
⑤	VALID (WAITING FOR SENDING, SENT)
S303	PRODUCE Ks1b
S304	OBTAIN KPcm1 FROM LOG MEMORY
S305	ENCRYPT Ks1b WITH KPcm1 TO PRODUCE E(KPcm1, Ks1b)
S306	PROVIDE E(KPcm1, Ks1b)
S307	ACCEPT E(KPcm1, Ks1b)
S308	PROVIDE E(KPcm1, Ks1b)
S309	ACCEPT E(KPcm1, Ks1b)
S310	DECRYPT E(KPcm1, Ks1b) WITH Kcm1 TO ACCEPT Ks1b
S311	PROVIDE LOG OUTPUT REQUEST
S312	ACCEPT LOG OUTPUT REQUEST
S313	LID OF DATA AT LBA STORED IN LOG MEMORY MATCHES WITH

LID STORED IN LOG MEMORY

⑥ MISMATCH

⑦ MATCH

S314 DATA AT LBA STORED IN LOG MEMORY IS VALID?

⑧ VALID

⑨ INVALID

S315 CHANGE ST2 IN LOG MEMORY TO "DATA PRESENT"

S316 CHANGE ST2 IN LOG MEMORY TO "SHIFTED"

S317 CHANGE ST2 IN LOG MEMORY TO "NO DATA"

S818 OBTAIN OUTPUT LOG (LID//Ks2a//ST1//ST2) FROM LOG MEMORY

S319 ENCRYPT Ks2c WITH Ks1b TO PRODUCE E(Ks1b, Ks2c)

S320 PRODUCE H(LID//E(Ks1b, Ks2c)//ST1//ST2)

S321 ENCRYPT H(LID//E(Ks1b, Ks2c)//ST1//ST2) WITH Ks1b TO PRODUCE E(Ks1b, H(LID//E(Ks1b, Ks2c)//ST1//ST2))

S322 PROVIDE LID//E(Ks1b, LID//ST1//ST2//E(Ks1b, H(LID//E(Ks1b, Ks2c)//ST1//ST2))

⑩ TO S323

⑪ TO S371

FIG. 17

① TERMINAL DEVICE 10

② FROM S322

③ FROM S302

S323 ACCEPT LID//E(Ks1b, LID//ST1//ST2//E(Ks1b, H(LID//E(Ks1b, Ks2c)//ST1//ST2))

S324 PROVIDE LID//E(Ks1b, LID//ST1//ST2//E(Ks1b, H(LID//E(Ks1b, Ks2c)//ST1//ST2))

S325 ACCEPT LID//E(Ks1b, LID//ST1//ST2//E(Ks1b, H(LID//E(Ks1b, Ks2c)//ST1//ST2))

S326 VERIFY LID//E(Ks1b, LID//ST1//ST2//E(Ks1b, H(LID//E(Ks1b, Ks2c)//ST1//ST2))

④ UNCERTIFIED

⑤ CERTIFIED

S327 CHECK LID

⑥ MISMATCH

⑦ MATCH

S328 DECRYPT E(Ks1b, Ks2c) WITH Ks1b TO ACCEPT Ks2c

S329 Ks2a: Ks2c

⑧ MISMATCH

⑨ MATCH

S330 CHECK RECEIVED ST1, ST2

⑩ ALREADY ACCEPTED

⑪ NOT ACCEPTED

S331 LID OF DATA AT LBA STORED IN LOG MEMORY MATCHES WITH LID STORED IN LOG MEMORY

⑫ MISMATCH

⑬ MATCH

S332 VALIDITY FLAG FOR LBA STORED IN LOG MEMORY

⑭ VALID

⑮ INVALID

S333 VALIDATE SEARCHED LICENSE

S334 PROVIDE LBA IN LOG MEMORY

⑯ TARGET OF REWRITE PROCESSING

S335 ACCEPT LBA

S336 PROVIDE SESSION KEY REQUEST

S337 PRODUCE SESSION KEY Ks2b

S338 STORE LID AND Ks2b IN LOG MEMORY
CHANGE ST1 TO "WAITING FOR RECEPTION"

S339 ENCRYPT Ks2b AND KPcm5 WITH Ks1b TO PRODUCE E(Ks1b, Ks2b//KPom5)

S340 PROVIDE LID//E(Ks1b, Ks2b//KPom5)

S341 ACCEPT LID//E(Ks1b, Ks2b//KPom5)

S342 PROVIDE LID//E(Ks1b, Ks2b//KPom5)

S343 ACCEPT LID//E(Ks1b, Ks2b//KPom5)

S344 DECRYPT E(Ks1b, Ks2b//KPom5) WITH Ks1b TO ACCEPT Ks2b AND KPom5

⑰ TO S371

⑱ TO S345

FIG. 18

① TERMINAL DEVICE 10

② FROM S302, S326, S327, S329-S331

③ FROM S344

S345 STORE LID AND Ks2b IN LOG MEMORY
CHANGE ST1 TO "WAITING FOR RECEPTION"

S346 PROVIDE STORAGE LBA OF TARGET LIC

④ TARGET OF REWRITE PROCESSING

S347 ACCEPT STORAGE LBA OF TARGET LIC

S348 STORE LBA IN LOG MEMORY

S349 VALIDITY FLAG FOR STORAGE LBA

⑤ INVALID

⑥ VALID

S350 OBTAIN LIC BASED ON LBA

S351	LID MATCH
⑦	MISMATCH
⑧	MATCH
S352	CHECK AC
⑨	PROHIBITED
S353	ENCRYPT LIC WITH KPom5 TO PRODUCE E(KPom5, LIC)
S354	ENCRYPT E(KPom5, LIC) WITH Ks2b TO PRODUCE E(Ks2b, E(KPom5, LIC))
S355	CHECK AC
⑩	COPY
⑪	SHIFT
S356	CHANGE VALIDITY FLAG FOR LBA TO "INVALID"
S357	CHANGE ST1 OF LOG MEMORY TO "SENT"
S358	PROVIDE E(Ks2b, E(KPom5, LIC))
S359	ACCEPT E(Ks2b, E(KPom5, LIC))
S360	PROVIDE E(Ks2b, E(KPom5, LIC))
S361	ACCEPT E(Ks2b, E(KPom5, LIC))
S362	DECRYPT E(Ks2b, E(KPom5, LIC)) WITH Ks2b TO ACCEPT E(KPom5, LIC)
S363	DECRYPT E(KPom5, LIC) WITH Kom5 TO ACCEPT LIC
S364	PROVIDE DESTINATION LBA OF LIC
S365	ACCEPT DESTINATION LBA OF LIC
S366	STORE DESTINATION LBA IN LOG MEMORY
S367	LID MATCH
⑫	MATCH
⑬	MISMATCH
S368	STORE LIC IN DESTINATION LBA
S369	CHANGE VALIDITY FLAG FOR DESTINATION LBA TO "VALID"

S370	CHANGE ST1 IN LOG MEMORY TO "RECEIVED"
S372	ISSUE ERROR NOTIFICATION
S373	ACCEPT ERROR NOTIFICATION
⑭	END DUE TO WRITE REJECTION
⑮	NORMAL END

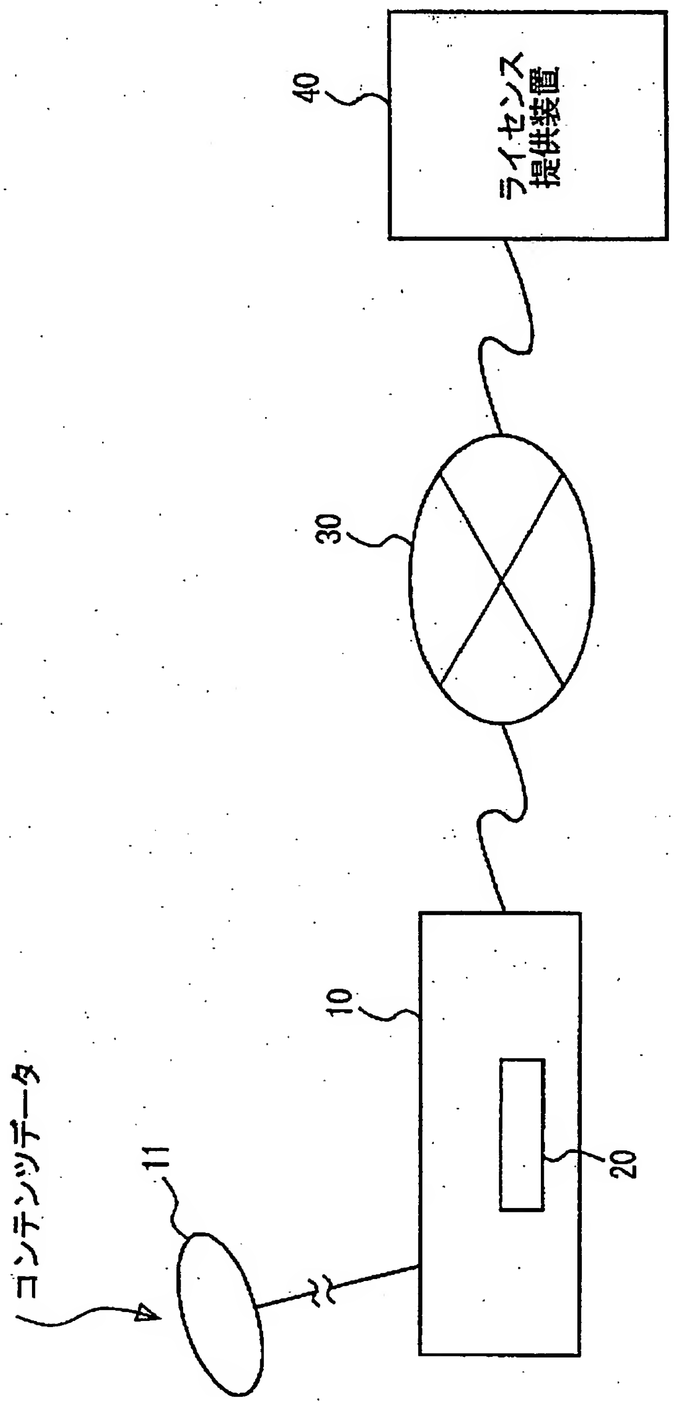
FIG. 19

①	REPRODUCING CIRCUIT 150
②	CONTROLLER 108
③	START
S401	ISSUE OUTPUT REQUEST FOR CERTIFICATE
S402	ACCEPT OUTPUT REQUEST FOR CERTIFICATE
S403	PROVIDE Cp3
S404	ACCEPT Cp3
S405	PROVIDE Cp3
S406	ACCEPT Cp3
S407	VERIFY Cp3
④	UNCERTIFIED
⑤	CERTIFIED
S408	ACCEPT KPcp3
S409	PRODUCE Ks1d
S410	ENCRYPT Ks1d WITH KPcp3 TO PRODUCE E(KPcp3, Ks1d)
S411	PROVIDE E(KPcp3, Ks1d)
S412	ACCEPT E(KPcp3, Ks1d)
S413	PROVIDE E(KPcp3, Ks1d)
S414	ACCEPT E(KPcp3, Ks1d)
S415	DECRYPT E(KPcp3, Ks1d) WITH Kcp3 TO ACCEPT Ks1d
S416	PRODUCE SESSION KEY Ks2d

S417	ENCRYPT Ks2d WITH Ks1d TO PRODUCE E(Ks1d, Ks2d)
S418	PROVIDE E(Ks1d, Ks2d)
S419	ACCEPT E(Ks1d, Ks2d)
S420	PROVIDE E(Ks1d, Ks2d)
S421	ACCEPT E(Ks1d, Ks2d)
S422	DECRYPT E(Ks1d, Ks2d) WITH Ks1d TO ACCEPT Ks2d
S423	PROVIDE STORAGE LBA OF TARGET LIC
S424	ACCEPT STORAGE LBA OF TARGET LIC
S425	VALIDITY FLAG FOR STORAGE LBA
⑥	INVALID
⑦	VALID
S426	OBTAIN LIC BASED ON STORAGE LBA
S427	CHECK AC
⑧	NO REPRODUCTION RESTRICTION
⑨	REPRODUCTION IS PROHIBITED
⑩	TIMES ARE LIMITED
S428	CHANGE AC OF STORAGE POSITION
S429	ENCRYPT Kc WITH Ks2d TO PRODUCE E(Ks2d, Kc)
S430	PROVIDE E(Ks2d, Kc)
S431	ACCEPT E(Ks2d, Kc)
S432	PROVIDE E(Ks2d, Kc)
S433	ACCEPT E(Ks2d, Kc)
S434	DECRYPT E(Ks2d, Kc) WITH Ks2d to ACCEPT Kc
S435	ISSUE ERROR NOTIFICATION
S436	ACCEPT ERROR NOTIFICATION
⑪	NORMAL END
⑫	END DUE TO REPRODUCTION REJECTION

【書類名】　図面

【図１】



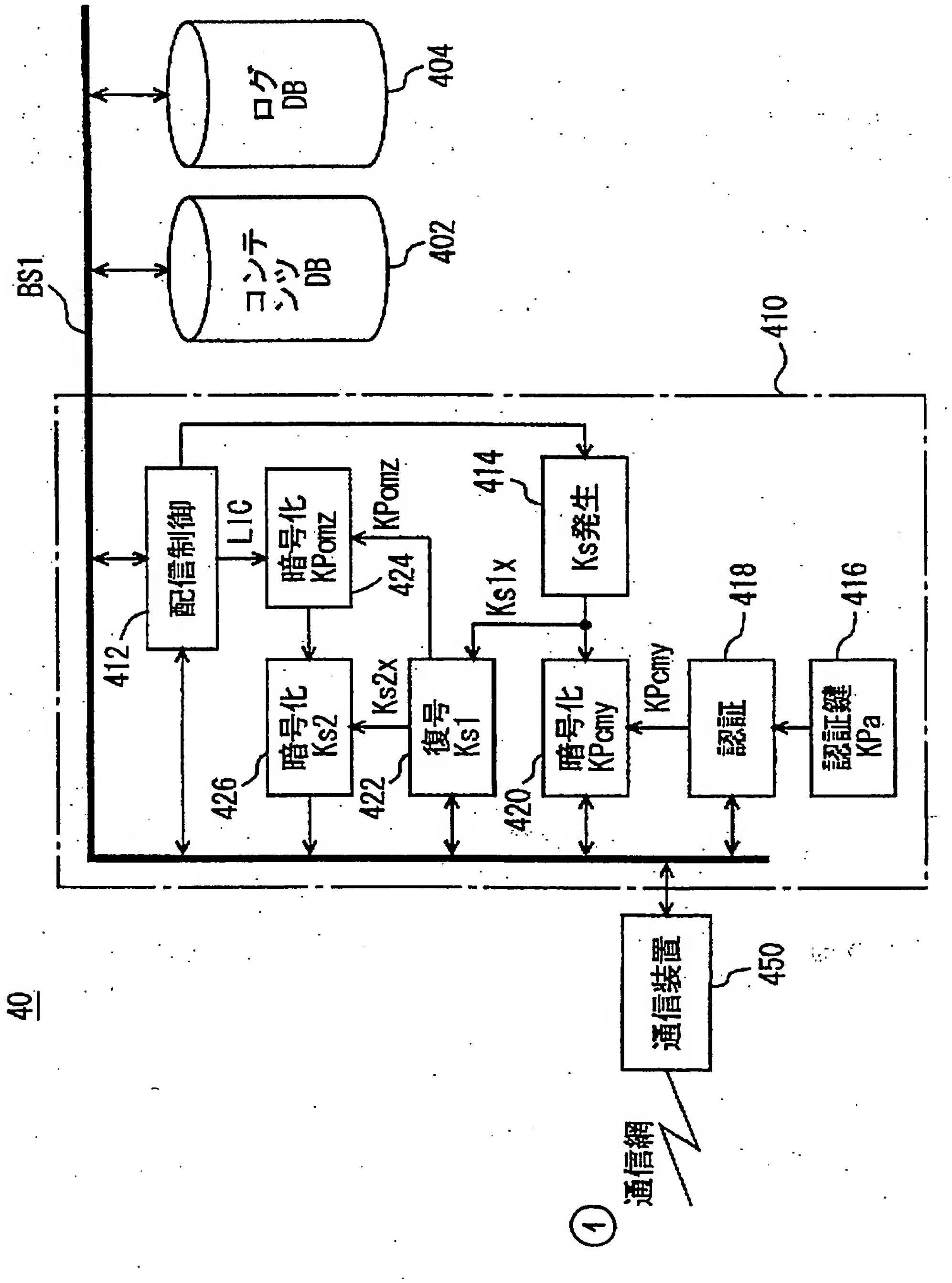
【図２】

記号	名称	属性	特性
Dc	データ	データ固有	例：映像データ、音楽データ、朗読データ、教材データ、 画像データ、ゲームプログラム Kcにて暗号化した暗号化コンテンツデータ E(Kc,Dc)として記録管理される
Di	データ情報	データ固有	Dcに付随する平文データ。DIDを含む
DID	データID	データ固有	DcおよびKcを特定するための管理コード
Kc	コンテンツ鍵	データ固有	暗号データを暗号／復号する共通鍵
AC	制御情報	ライセンス固有	再生やライセンスの取扱いに関する制限事項
LID	ライセンスID	ライセンス固有	ライセンスを特定するための管理コード
LIC	ライセンス	ライセンス固有	Kc//AC//DID//LIDの総称

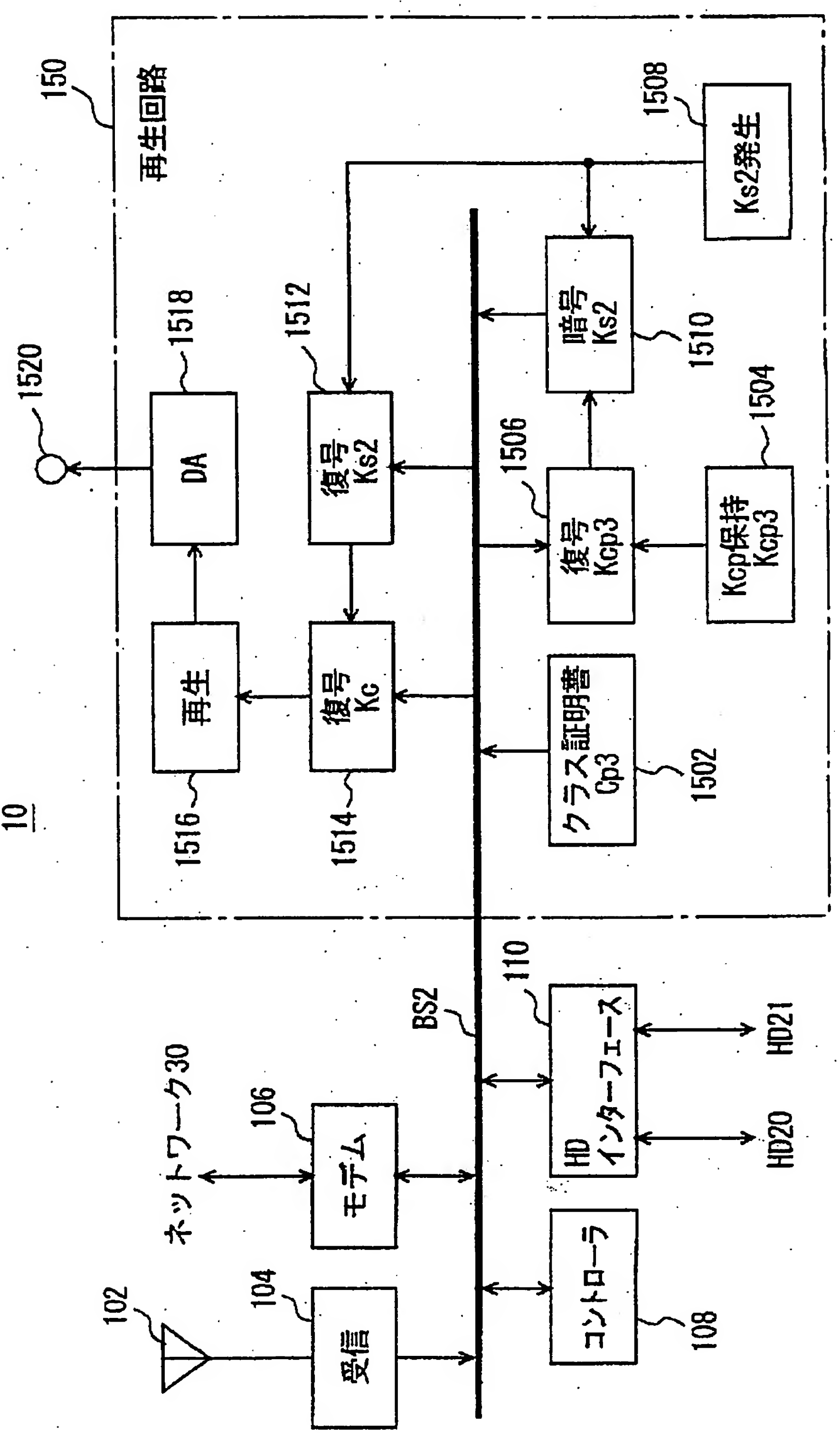
【図３】

	記号	名称	特性
ライセンス提供装置	KPa	認証鍵	認証局にて証明書を検証する公開復号鍵 ライセンス提供側にて運用される
	Ks1x	セッション鍵	ライセンスの配信ごとに生成される一時鍵 共通鍵
データ記録装置 (ハードディスク)	Ka	マスタ鍵	クラス証明書作成のために使用する秘密暗号鍵 認証局にて運用される
	KPa	認証鍵	認証局にて証明書を検証する公開復号鍵 ライセンス提供側にて運用される
	KPcmy	クラス公開鍵	機器のクラス(種類などの一定の単位ごと)に付与される暗号鍵 「y」はクラスを識別するための識別子
	Kcmy	クラス秘密鍵	クラス公開鍵KPcmyにて暗号化されたデータを復号する非対称な復号鍵
	Icmy	クラス情報	クラスごとの機器およびクラス公開鍵に関する情報データ
	Cmy	クラス証明書	Cmy=KPcmy//Icmy//E(Ka,H(KPcmy//Icmy)) 認証鍵KPaによってその正当性が確認できる
	KPcmz	個別公開鍵	データ記録装置ごとに固有な値を持つ個別公開暗号鍵 「z」はデータ記録装置を識別するための識別子
	Kcmz	個別秘密鍵	個別公開鍵KPcmzにて暗号化されたデータを復号する非対称な復号鍵
	Ks1x	セッション鍵	ライセンスの授受ごとにライセンス提供側で生成される一時鍵 共通鍵
	Ks2x	セッション鍵	ライセンスの授受ごとにライセンス受理側で生成される一時鍵 共通鍵
再生回路	KPcpy	クラス公開鍵	機器のクラス(種類などの一定の単位ごと)に付与される暗号鍵 「y」はクラスを識別するための識別子
	Kcpy	クラス秘密鍵	クラス公開鍵KPcpyにて暗号化されたデータを復号する非対称な復号鍵
	Icpy	クラス情報	クラスごとの機器およびクラス公開鍵に関する情報データ
	Cpy	クラス証明書	Cpy=KPcpy//Icpy//E(Ka,H(KPcpy//Icpy)) 認証鍵KPaによってその正当性が確認できる
	Ks2x	セッション鍵	ライセンスの授受ごとにライセンス受理側で生成される一時鍵 共通鍵

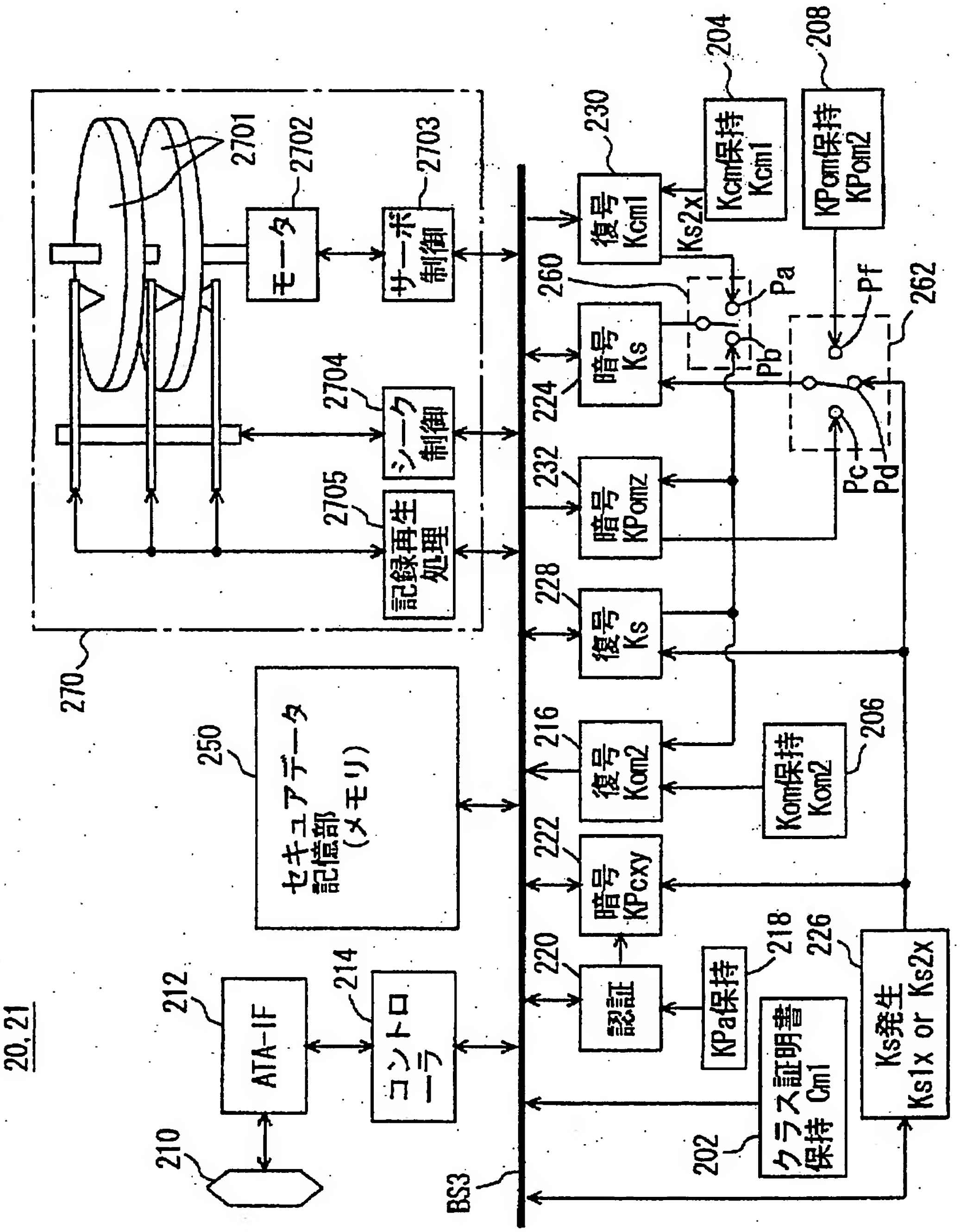
【図４】


ログ
DB
404
コンテンツ
DB
402
BS1
410
配信制御
412
LIC
暗号化
KPomz
KPomz
424
Ks発生
414
Ks1x
暗号化
Ks2
426
Ks2x
復号
Ks1
422
暗号化
KPcmy
420
KPcmy
認証
418
認証鍵
KPa
416
通信装置
450
通信網
①
40

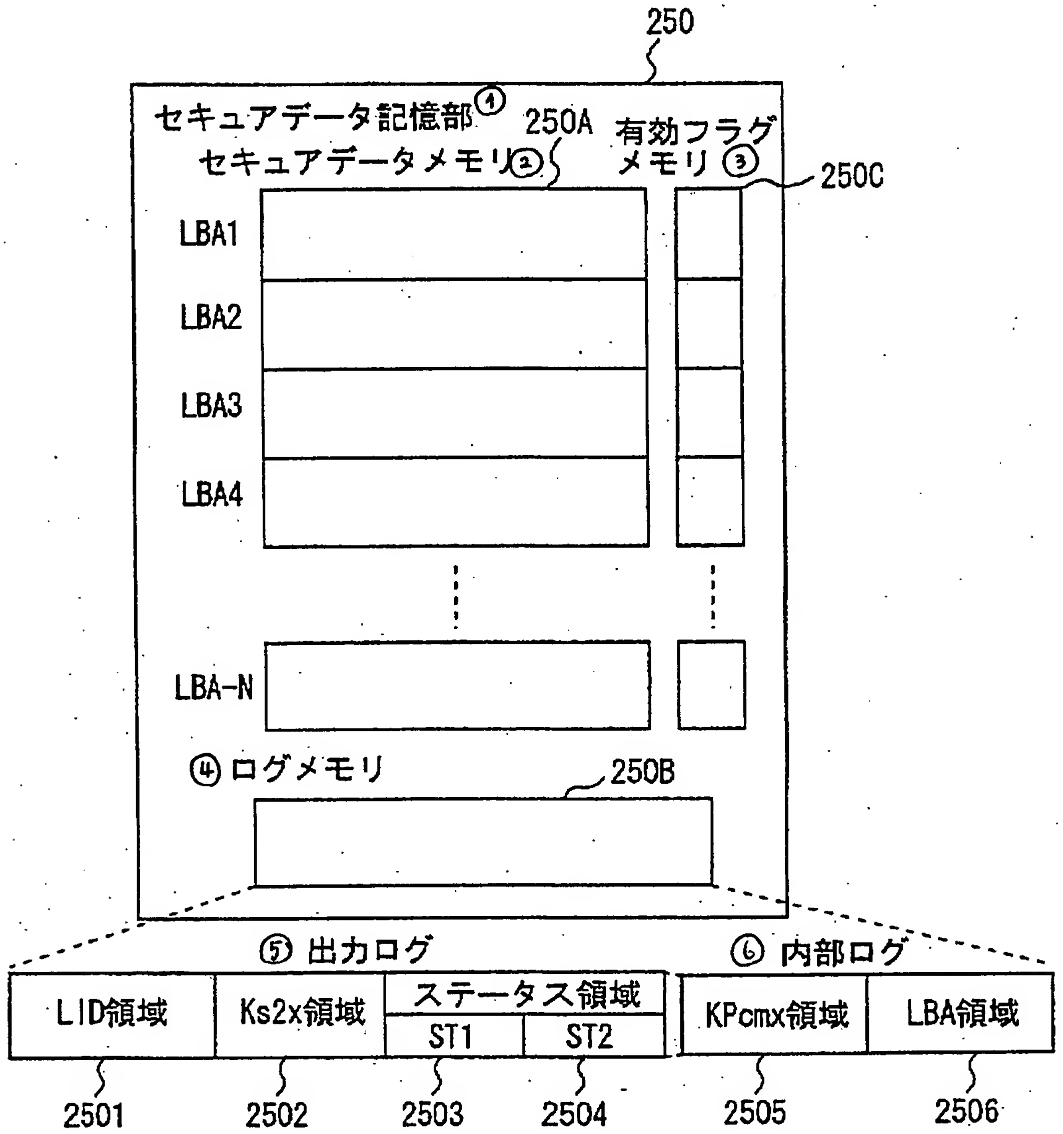
【図５】


10
150
再生回路
1508
Ks2発生
1510
暗号 Ks2
1504
Kcp保持 Kcp3
1506
復号 Kcp3
1502
クラス証明書 Cp3
1512
復号 Ks2
1514
復号 Kc
1518
DA
1520
1516
再生
BS2
110
HD インターフェース
HD21
HD20
106
モデム
ネットワーク30
104
受信
102
コントローラ
108

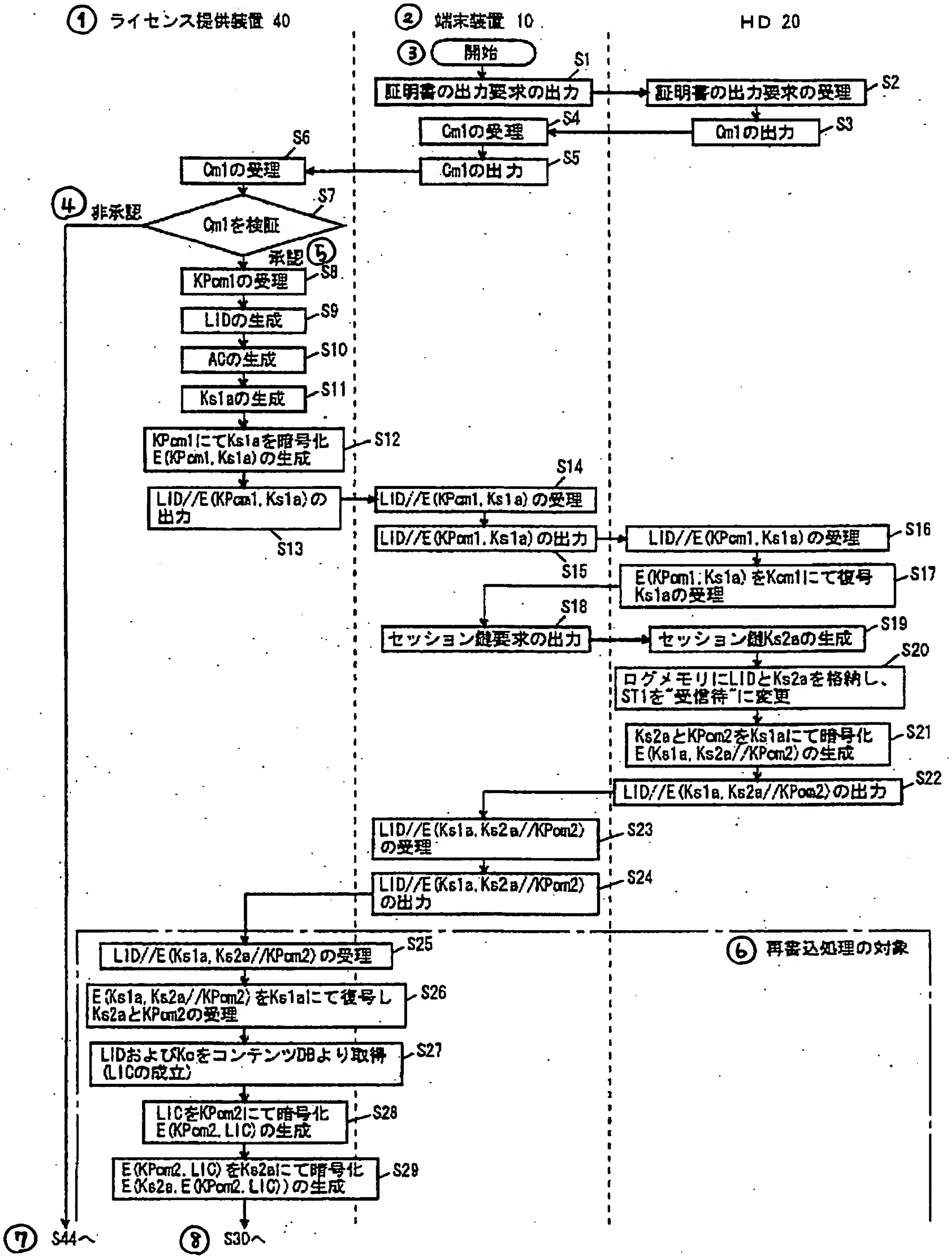
【図６】


20,21
210
212
ATA-IF
214
コントローラ
BS3
250
セキュアデータ記憶部（メモリ）
270
2701
2702
モータ
2703
サーボ制御
2704
シーク制御
2705
記録再生処理
202
クラス証明書保持 Cm1
218
KPa保持
220
認証
222
暗号 KPcxy
226
Ks発生 Ks1x or Ks2x
216
復号 Kcm2
206
Kcm保持 Kcm2
228
復号 Ks
232
暗号 KPcmz
224
暗号 Ks
230
復号 Kcm1
204
Kcm保持 Kcm1
208
KPcm保持 KPcm2
Ks2x
260
Pa
Pb
262
Pf
Pc
Pd

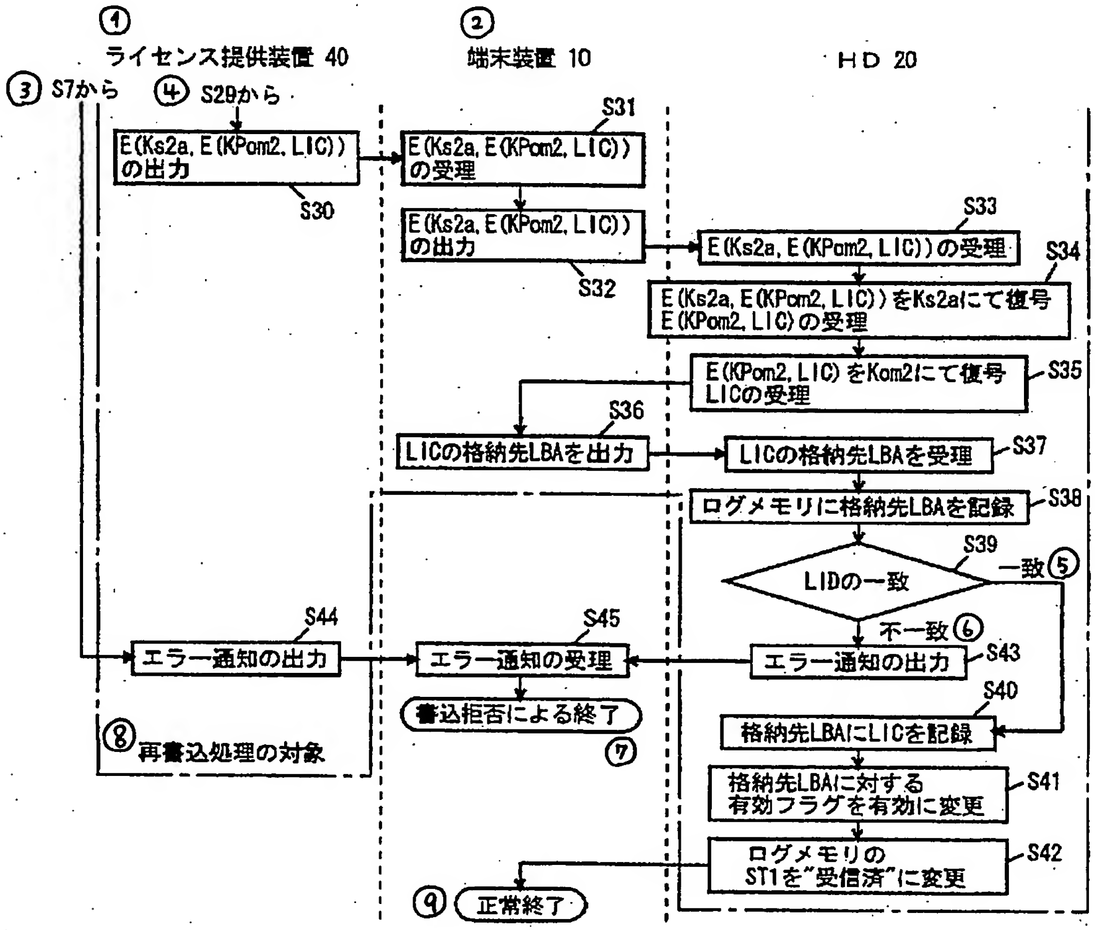
【図７】


250
セキュアデータ記憶部①
250A
セキュアデータメモリ②
有効フラグメモリ③
250C
LBA1
LBA2
LBA3
LBA4
LBA-N
④ログメモリ
250B
⑤出力ログ
LID領域
Ks2x領域
ステータス領域
ST1
ST2
⑥内部ログ
KPcmx領域
LBA領域
2501
2502
2503
2504
2505
2506

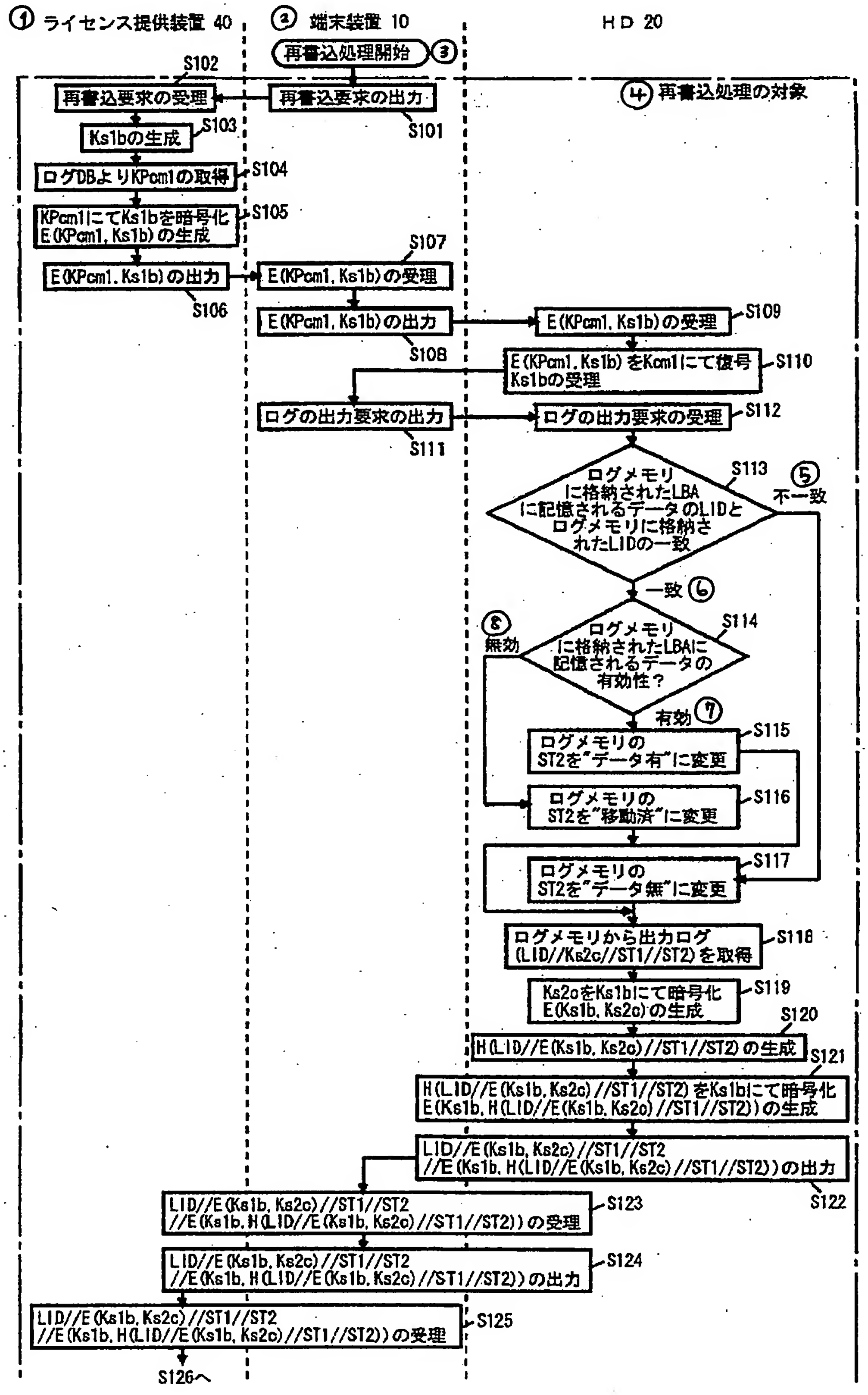
【図８】


① ライセンス提供装置 40
② 端末装置 10
HD 20
③ 開始
S1
証明書の出力要求の出力
証明書の出力要求の受理
S2
Cm1の出力
S3
Cm1の受理
S4
Cm1の出力
S5
S6
Cm1の受理
S7
Cm1を検証
④ 非承認
承認 ⑤
KPcm1の受理
S8
LIDの生成
S9
ACの生成
S10
Ks1aの生成
S11
KPcm1にてKs1aを暗号化
E(KPcm1, Ks1a)の生成
S12
LID//E(KPcm1, Ks1a)の出力
S13
S14
LID//E(KPcm1, Ks1a)の受理
LID//E(KPcm1, Ks1a)の出力
S15
LID//E(KPcm1, Ks1a)の受理
S16
E(KPcm1 ; Ks1a)をKcm1にて復号
Ks1aの受理
S17
S18
セッション鍵要求の出力
セッション鍵Ks2aの生成
S19
S20
ログメモリにLIDとKs2aを格納し、
ST1を"受信待"に変更
Ks2aとKPcm2をKs1aにて暗号化
E(Ks1a, Ks2a//KPcm2)の生成
S21
LID//E(Ks1a, Ks2a//KPcm2)の出力
S22
LID//E(Ks1a, Ks2a//KPcm2)
の受理
S23
LID//E(Ks1a, Ks2a//KPcm2)
の出力
S24
⑥ 再書込処理の対象
LID//E(Ks1a, Ks2a//KPcm2)の受理
S25
E(Ks1a, Ks2a//KPcm2)をKs1aにて復号し
Ks2aとKPcm2の受理
S26
LIDおよびKcをコンテンツDBより取得
(LICの成立)
S27
LICをKPcm2にて暗号化
E(KPcm2, LIC)の生成
S28
E(KPcm2, LIC)をKs2aにて暗号化
E(Ks2a, E(KPcm2, LIC))の生成
S29
⑦ S44へ
⑧ S30へ

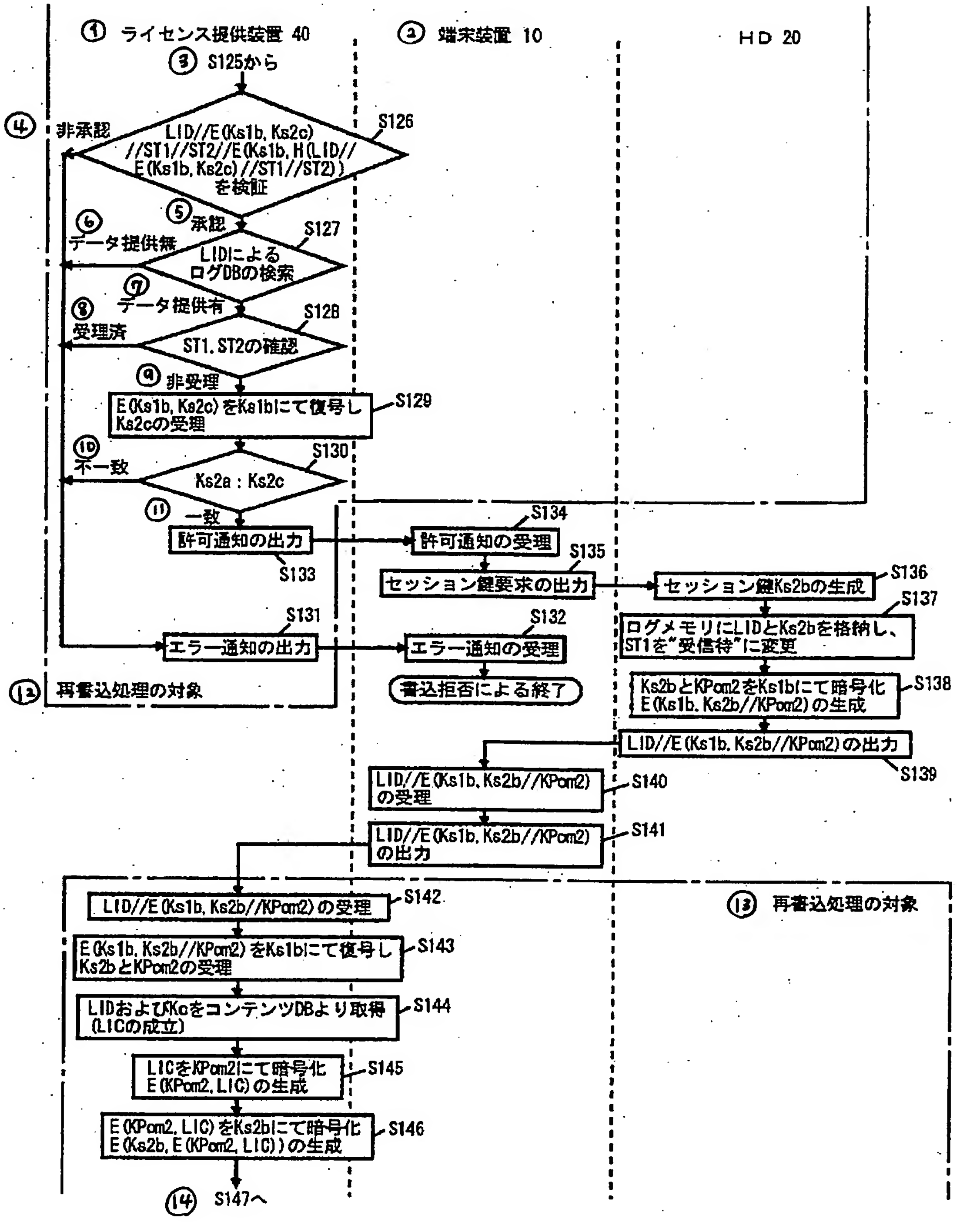
【図９】


①
ライセンス提供装置 40
②
端末装置 10
HD 20
③ S7から
④ S29から
E(Ks2a, E(KPom2, LIC))の出力
S30
S31
E(Ks2a, E(KPom2, LIC))の受理
E(Ks2a, E(KPom2, LIC))の出力
S32
S33
E(Ks2a, E(KPom2, LIC))の受理
S34
E(Ks2a, E(KPom2, LIC))をKs2aにて復号
E(KPom2, LIC)の受理
E(KPom2, LIC)をKom2にて復号
LICの受理
S35
S36
LICの格納先LBAを出力
LICの格納先LBAを受理
S37
ログメモリに格納先LBAを記録
S38
S39
LIDの一致
一致⑤
不一致⑥
S44
エラー通知の出力
S45
エラー通知の受理
エラー通知の出力
S43
書込拒否による終了
⑦
⑧再書込処理の対象
S40
格納先LBAにLICを記録
格納先LBAに対する
有効フラグを有効に変更
S41
ログメモリの
ST1を"受信済"に変更
S42
⑨ 正常終了

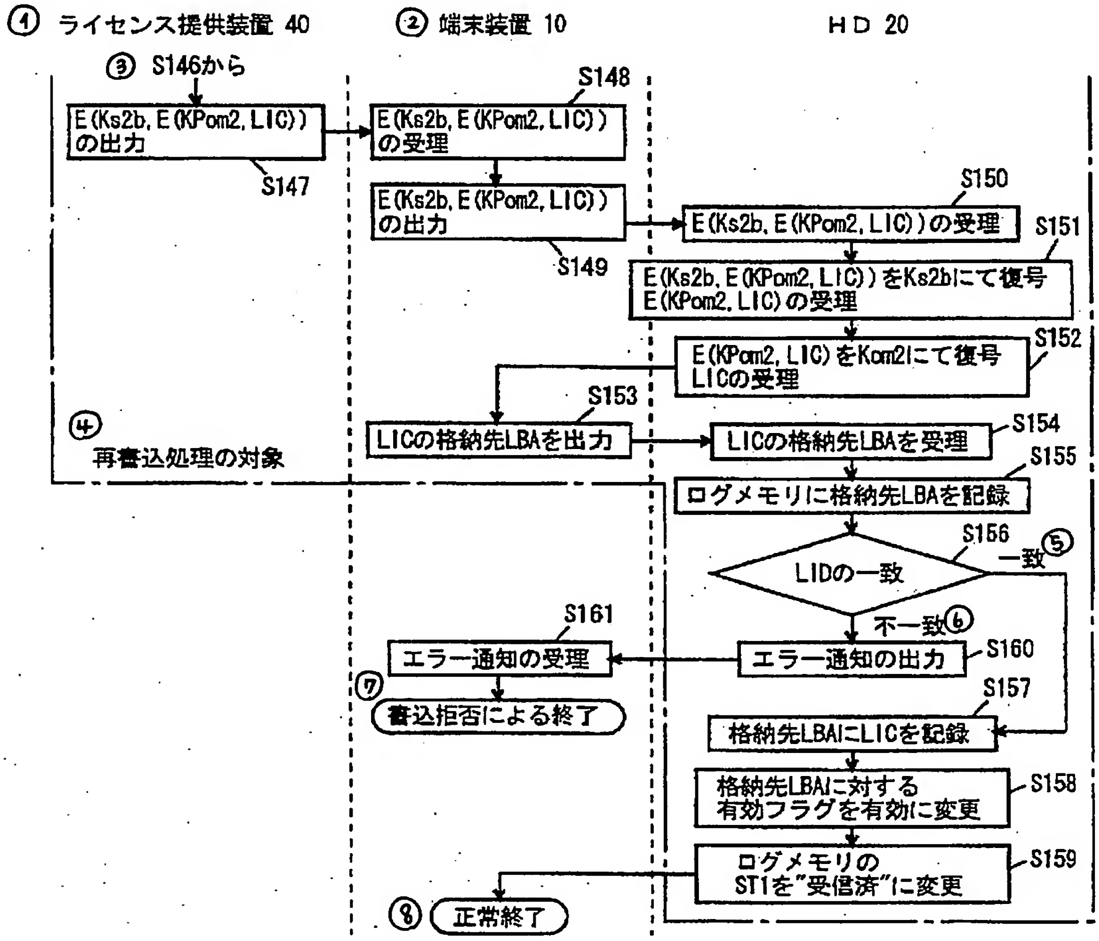
【図１０】


① ライセンス提供装置 40
② 端末装置 10
HD 20
再書込処理開始 ③
④ 再書込処理の対象
S102
再書込要求の受理
再書込要求の出力
S101
Ks1bの生成
S103
ログDBよりKPcm1の取得
S104
KPcm1にてKs1bを暗号化
E(KPcm1, Ks1b) の生成
S105
S107
E(KPcm1. Ks1b) の出力
E(KPcm1, Ks1b) の受理
S106
E(KPcm1, Ks1b) の出力
E(KPcm1, Ks1b) の受理
S109
S108
E(KPcm1, Ks1b) をKcm1にて復号
Ks1bの受理
S110
ログの出力要求の出力
ログの出力要求の受理
S112
S111
ログメモリ
に格納されたLBA
に記憶されるデータのLIDと
ログメモリに格納さ
れたLIDの一致
S113
⑤ 不一致
一致 ⑥
⑧ 無効
ログメモリ
に格納されたLBAに
記憶されるデータの
有効性？
S114
有効 ⑦
ログメモリの
ST2を"データ有"に変更
S115
ログメモリの
ST2を"移動済"に変更
S116
ログメモリの
ST2を"データ無"に変更
S117
ログメモリから出力ログ
(LID//Ks2c//ST1//ST2) を取得
S118
Ks2cをKs1bにて暗号化
E(Ks1b, Ks2c) の生成
S119
S120
H(LID//E(Ks1b, Ks2c)//ST1//ST2) の生成
S121
H(LID//E(Ks1b, Ks2c)//ST1//ST2) をKs1bにて暗号化
E(Ks1b, H(LID//E(Ks1b, Ks2c)//ST1//ST2)) の生成
LID//E(Ks1b, Ks2c)//ST1//ST2
//E(Ks1b, H(LID//E(Ks1b, Ks2c)//ST1//ST2)) の出力
S122
LID//E(Ks1b, Ks2c)//ST1//ST2
//E(Ks1b, H(LID//E(Ks1b, Ks2c)//ST1//ST2)) の受理
S123
LID//E(Ks1b, Ks2c)//ST1//ST2
//E(Ks1b, H(LID//E(Ks1b, Ks2c)//ST1//ST2)) の出力
S124
LID//E(Ks1b, Ks2c)//ST1//ST2
//E(Ks1b, H(LID//E(Ks1b, Ks2c)//ST1//ST2)) の受理
S125
S126へ

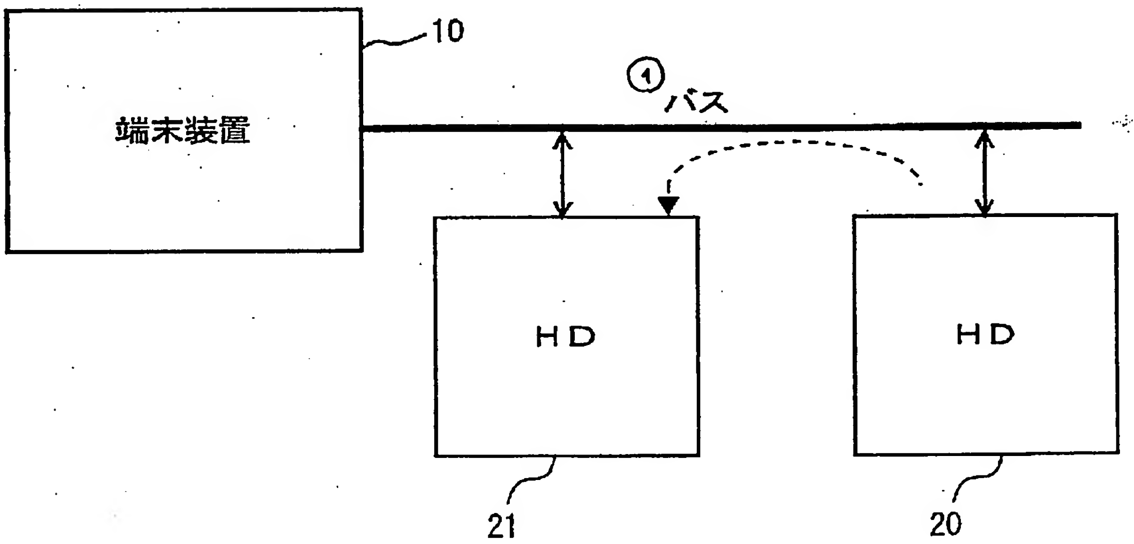
【図１１】


① ライセンス提供装置 40
② 端末装置 10
HD 20
③ S125から
④ 非承認
LID//E(Ks1b, Ks2c)//ST1//ST2//E(Ks1b, H(LID//E(Ks1b, Ks2c)//ST1//ST2))を検証
S126
⑤ 承認
⑥ データ提供無
LIDによるログDBの検索
S127
⑦ データ提供有
⑧ 受理済
ST1, ST2の確認
S128
⑨ 非受理
E(Ks1b, Ks2c)をKs1bにて復号しKs2cの受理
S129
⑩ 不一致
Ks2a : Ks2c
S130
⑪ 一致
許可通知の出力
S133
許可通知の受理
S134
セッション鍵要求の出力
S135
セッション鍵Ks2bの生成
S136
ログメモリにLIDとKs2bを格納し、ST1を"受信待"に変更
S137
Ks2bとKPom2をKs1bにて暗号化E(Ks1b, Ks2b//KPom2)の生成
S138
LID//E(Ks1b, Ks2b//KPom2)の出力
S139
S131
エラー通知の出力
S132
エラー通知の受理
書込拒否による終了
⑫ 再書込処理の対象
LID//E(Ks1b, Ks2b//KPom2)の受理
S140
LID//E(Ks1b, Ks2b//KPom2)の出力
S141
LID//E(Ks1b, Ks2b//KPom2)の受理
S142
⑬ 再書込処理の対象
E(Ks1b, Ks2b//KPom2)をKs1bにて復号しKs2bとKPom2の受理
S143
LIDおよびKcをコンテンツDBより取得(LICの成立)
S144
LICをKPom2にて暗号化E(KPom2, LIC)の生成
S145
E(KPom2, LIC)をKs2bにて暗号化E(Ks2b, E(KPom2, LIC))の生成
S146
⑭ S147へ

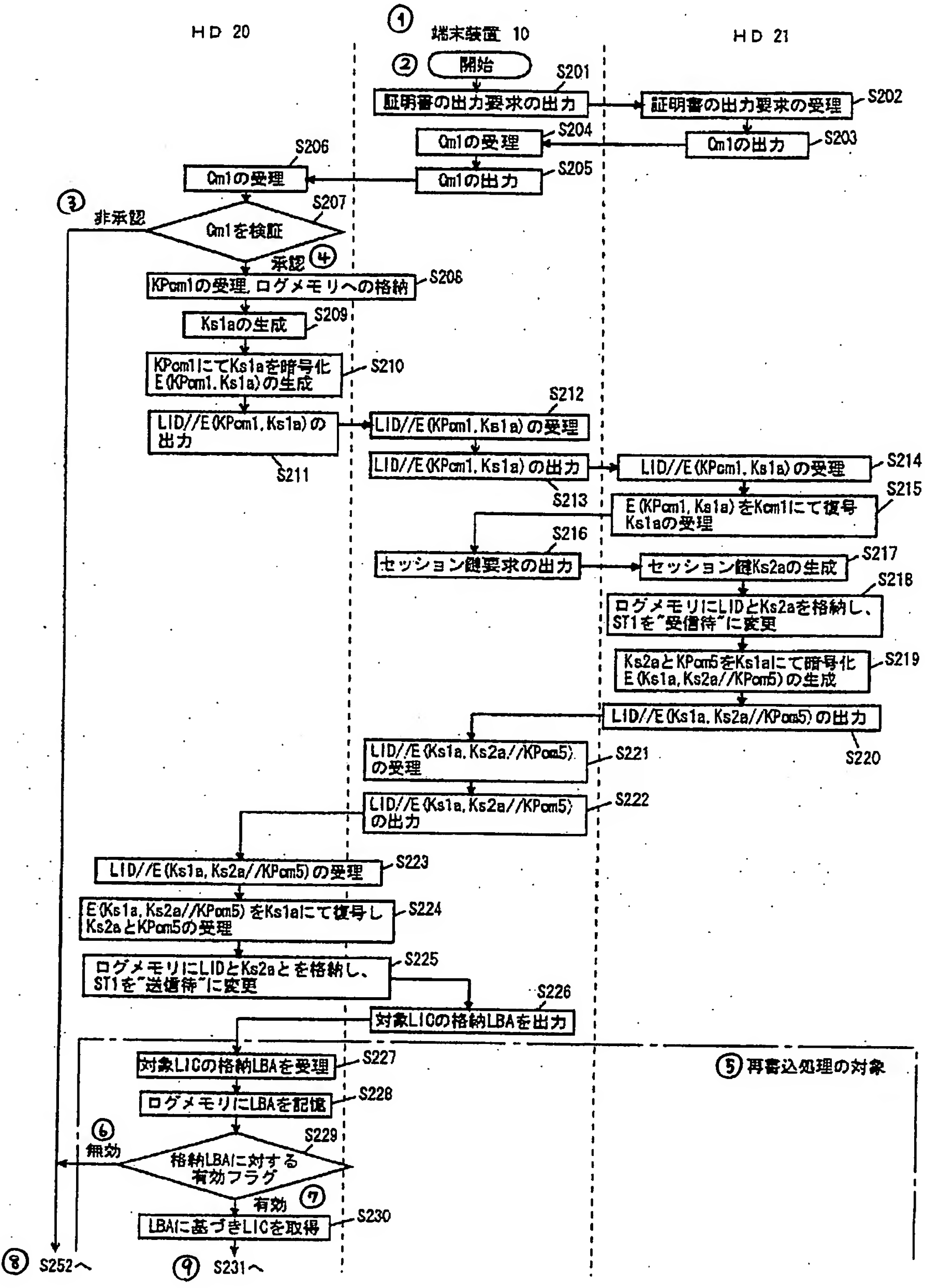
【図１２】


④ ライセンス提供装置 40
② 端末装置 10
ＨＤ 20
③ S146から
E(Ks2b, E(KPom2, LIC))の出力
S147
S148
E(Ks2b, E(KPom2, LIC))の受理
E(Ks2b, E(KPom2, LIC))の出力
S149
S150
E(Ks2b, E(KPom2, LIC))の受理
S151
E(Ks2b, E(KPom2, LIC))をKs2bにて復号 E(KPom2, LIC)の受理
S152
E(KPom2, LIC)をKom2にて復号 LICの受理
S153
LICの格納先LBAを出力
S154
LICの格納先LBAを受理
④ 再書込処理の対象
S155
ログメモリに格納先LBAを記録
S156
LIDの一致
一致⑤
不一致⑥
S161
エラー通知の受理
エラー通知の出力
S160
⑦
書込拒否による終了
S157
格納先LBAにLICを記録
格納先LBAに対する 有効フラグを有効に変更
S158
ログメモリの ST1を"受信済"に変更
S159
⑧ 正常終了

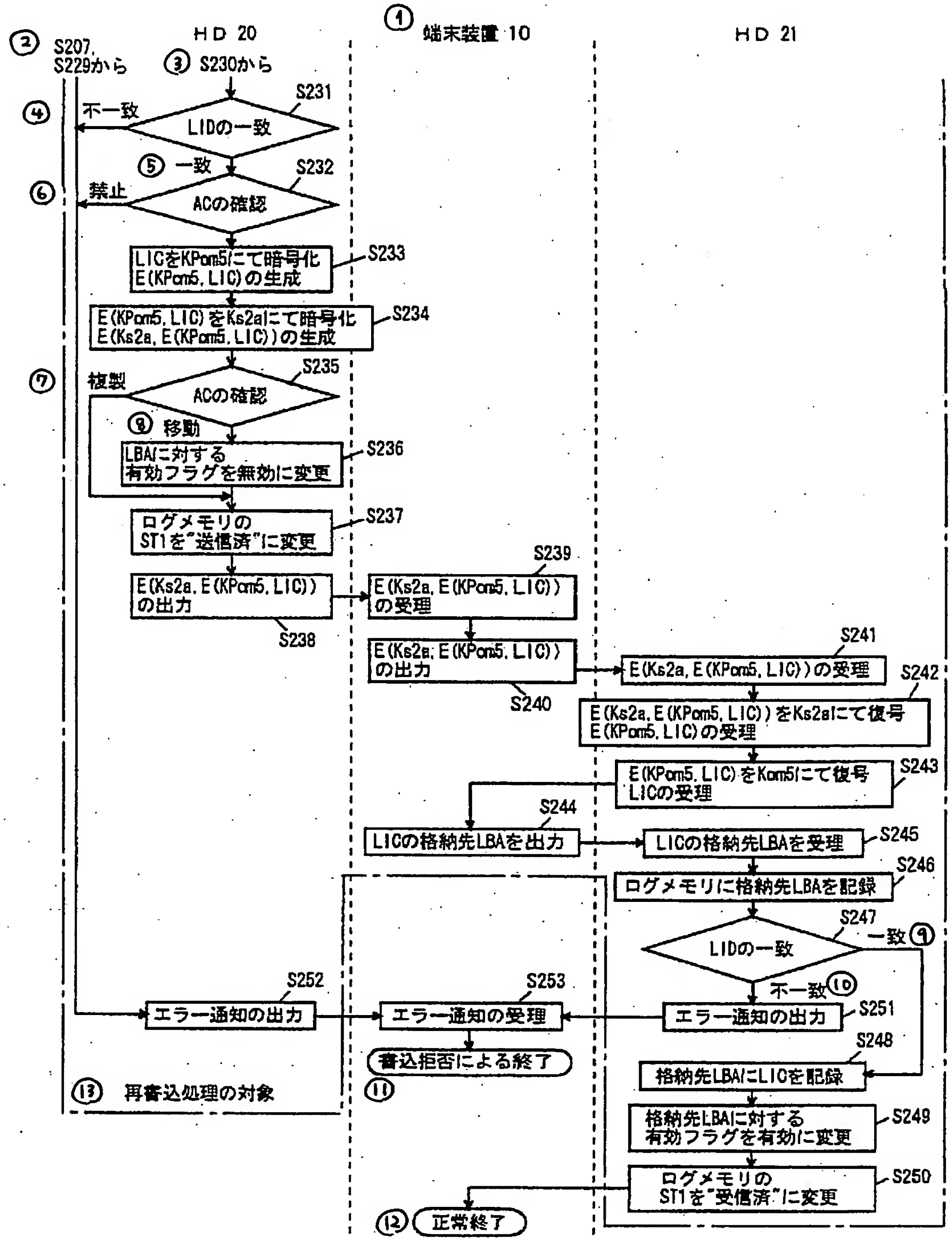
【図１３】


10
端末装置
① バス
ＨＤ
ＨＤ
21
20

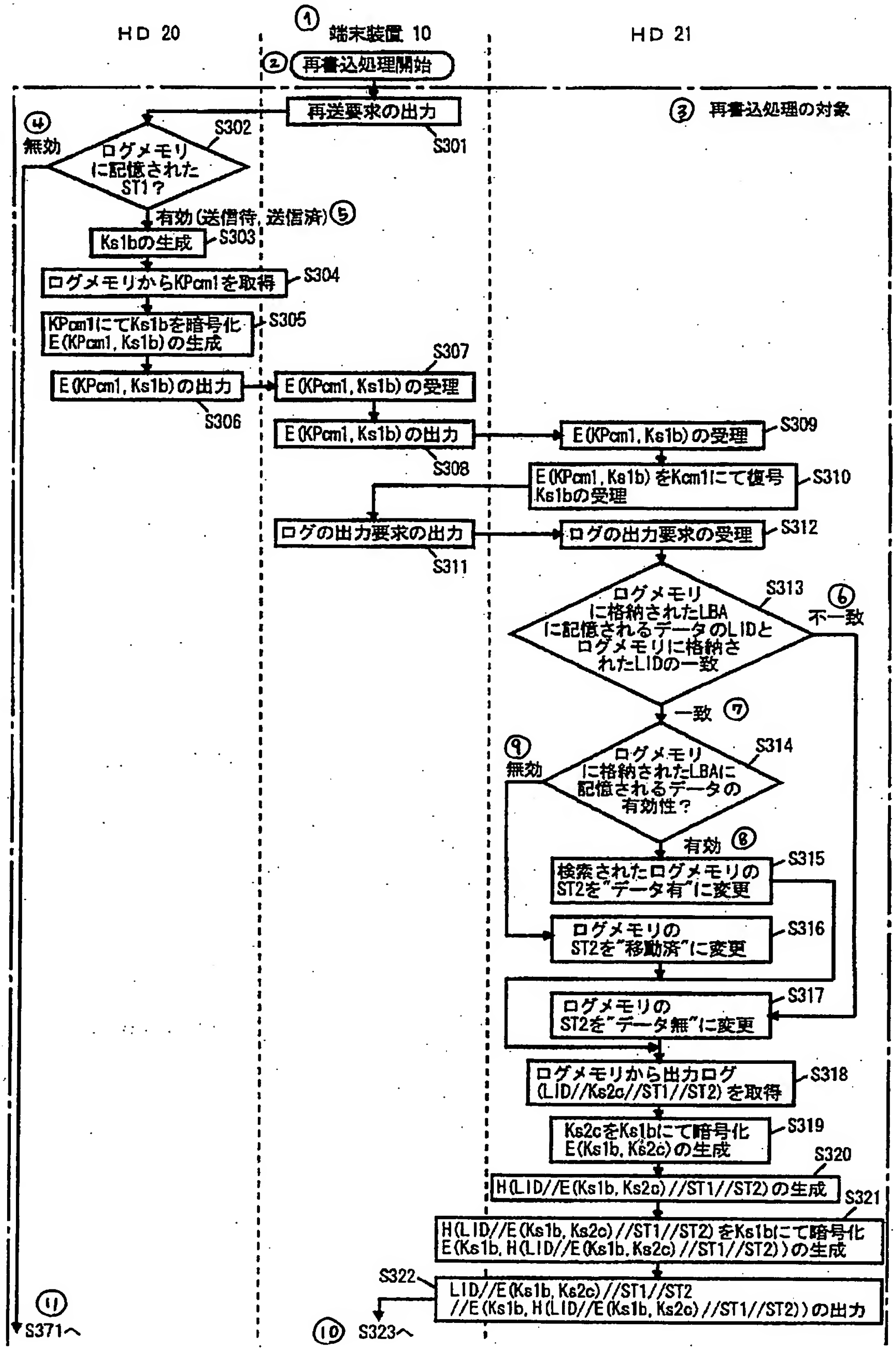
【図１４】


HD 20
① 端末装置 10
HD 21
② 開始
S201
証明書の出力要求の出力
証明書の出力要求の受理
S202
Cm1の出力
S203
Cm1の受理
S204
Cm1の出力
S205
Cm1の受理
S206
③ 非承認
Cm1を検証
S207
承認 ④
KPcm1の受理，ログメモリへの格納
S208
Ks1aの生成
S209
KPcm1にてKs1aを暗号化
E(KPcm1，Ks1a)の生成
S210
LID//E(KPcm1，Ks1a)の出力
S211
LID//E(KPcm1，Ks1a)の受理
S212
LID//E(KPcm1，Ks1a)の出力
S213
LID//E(KPcm1，Ks1a)の受理
S214
E(KPcm1，Ks1a)をKcm1にて復号
Ks1aの受理
S215
セッション鍵要求の出力
S216
セッション鍵Ks2aの生成
S217
ログメモリにLIDとKs2aを格納し、
ST1を"受信待"に変更
S218
Ks2aとKPcm5をKs1aにて暗号化
E(Ks1a，Ks2a//KPcm5)の生成
S219
LID//E(Ks1a，Ks2a//KPcm5)の出力
S220
LID//E(Ks1a，Ks2a//KPcm5)の受理
S221
LID//E(Ks1a，Ks2a//KPcm5)の出力
S222
LID//E(Ks1a，Ks2a//KPcm5)の受理
S223
E(Ks1a，Ks2a//KPcm5)をKs1aにて復号し
Ks2aとKPcm5の受理
S224
ログメモリにLIDとKs2aとを格納し、
ST1を"送信待"に変更
S225
対象LICの格納LBAを出力
S226
対象LICの格納LBAを受理
S227
⑤ 再書込処理の対象
ログメモリにLBAを記憶
S228
⑥ 無効
格納LBAに対する
有効フラグ
S229
有効 ⑦
LBAに基づきLICを取得
S230
⑧ S252へ
⑨ S231へ

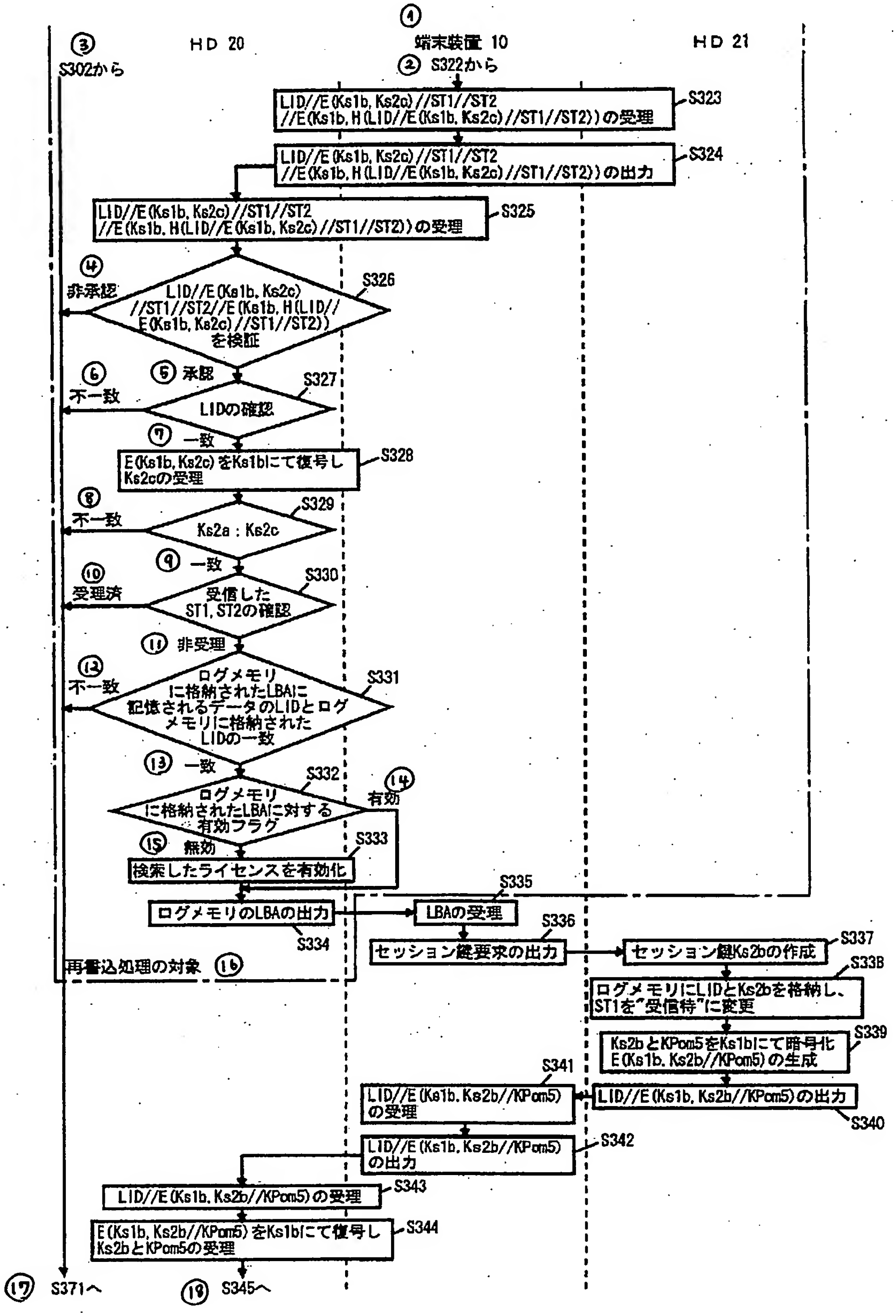
【図１５】


①
端末装置 10
HD 20
HD 21
②
S207,
S229から
③
S230から
S231
LIDの一致
④
不一致
⑤
一致
S232
ACの確認
⑥
禁止
S233
LICをKPom5にて暗号化
E(KPom5, LIC)の生成
S234
E(KPom5, LIC)をKs2aにて暗号化
E(Ks2a, E(KPom5, LIC))の生成
S235
ACの確認
⑦
複製
⑧
移動
S236
LBAに対する
有効フラグを無効に変更
S237
ログメモリの
ST1を"送信済"に変更
E(Ks2a, E(KPom5, LIC))
の出力
S238
S239
E(Ks2a, E(KPom5, LIC))
の受理
E(Ks2a, E(KPom5, LIC))
の出力
S240
S241
E(Ks2a, E(KPom5, LIC))の受理
S242
E(Ks2a, E(KPom5, LIC))をKs2aにて復号
E(KPom5, LIC)の受理
S243
E(KPom5, LIC)をKom5にて復号
LICの受理
S244
LICの格納先LBAを出力
LICの格納先LBAを受理
S245
S246
ログメモリに格納先LBAを記録
S247
LIDの一致
一致
⑨
不一致
⑩
S252
エラー通知の出力
S253
エラー通知の受理
エラー通知の出力
S251
書込拒否による終了
⑪
S248
格納先LBAにLICを記録
格納先LBAに対する
有効フラグを有効に変更
S249
ログメモリの
ST1を"受信済"に変更
S250
⑫
正常終了
⑬
再書込処理の対象

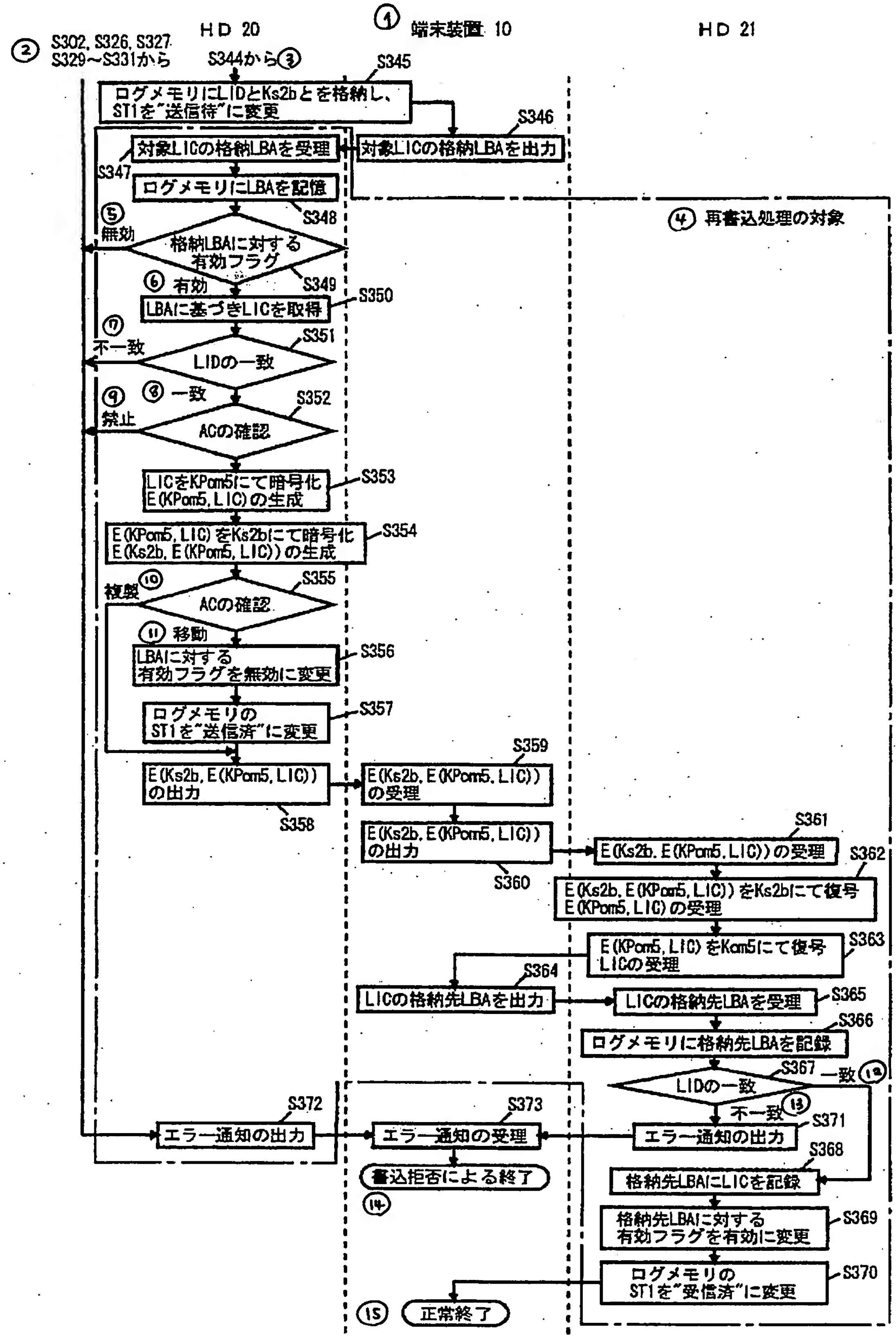
【図１６】


HD 20
①
端末装置 10
HD 21
②
再書込処理開始
③ 再書込処理の対象
再送要求の出力
S301
④
無効
ログメモリに記憶されたST1？
S302
有効(送信待, 送信済)⑤
Ks1bの生成
S303
ログメモリからKPcm1を取得
S304
KPcm1にてKs1bを暗号化
E(KPcm1, Ks1b)の生成
S305
E(KPcm1, Ks1b)の出力
S306
E(KPcm1, Ks1b)の受理
S307
E(KPcm1, Ks1b)の出力
S308
E(KPcm1, Ks1b)の受理
S309
E(KPcm1, Ks1b)をKcm1にて復号
Ks1bの受理
S310
ログの出力要求の出力
S311
ログの出力要求の受理
S312
ログメモリに格納されたLBAに記憶されるデータのLIDとログメモリに格納されたLIDの一致
S313
⑥
不一致
一致 ⑦
⑨
無効
ログメモリに格納されたLBAに記憶されるデータの有効性？
S314
有効 ⑧
検索されたログメモリのST2を"データ有"に変更
S315
ログメモリのST2を"移動済"に変更
S316
ログメモリのST2を"データ無"に変更
S317
ログメモリから出力ログ(LID//Ks2c//ST1//ST2)を取得
S318
Ks2cをKs1bにて暗号化
E(Ks1b, Ks2c)の生成
S319
H(LID//E(Ks1b, Ks2c)//ST1//ST2)の生成
S320
H(LID//E(Ks1b, Ks2c)//ST1//ST2)をKs1bにて暗号化
E(Ks1b, H(LID//E(Ks1b, Ks2c)//ST1//ST2))の生成
S321
S322
LID//E(Ks1b, Ks2c)//ST1//ST2
//E(Ks1b, H(LID//E(Ks1b, Ks2c)//ST1//ST2))の出力
⑪
S371へ
⑩ S323へ

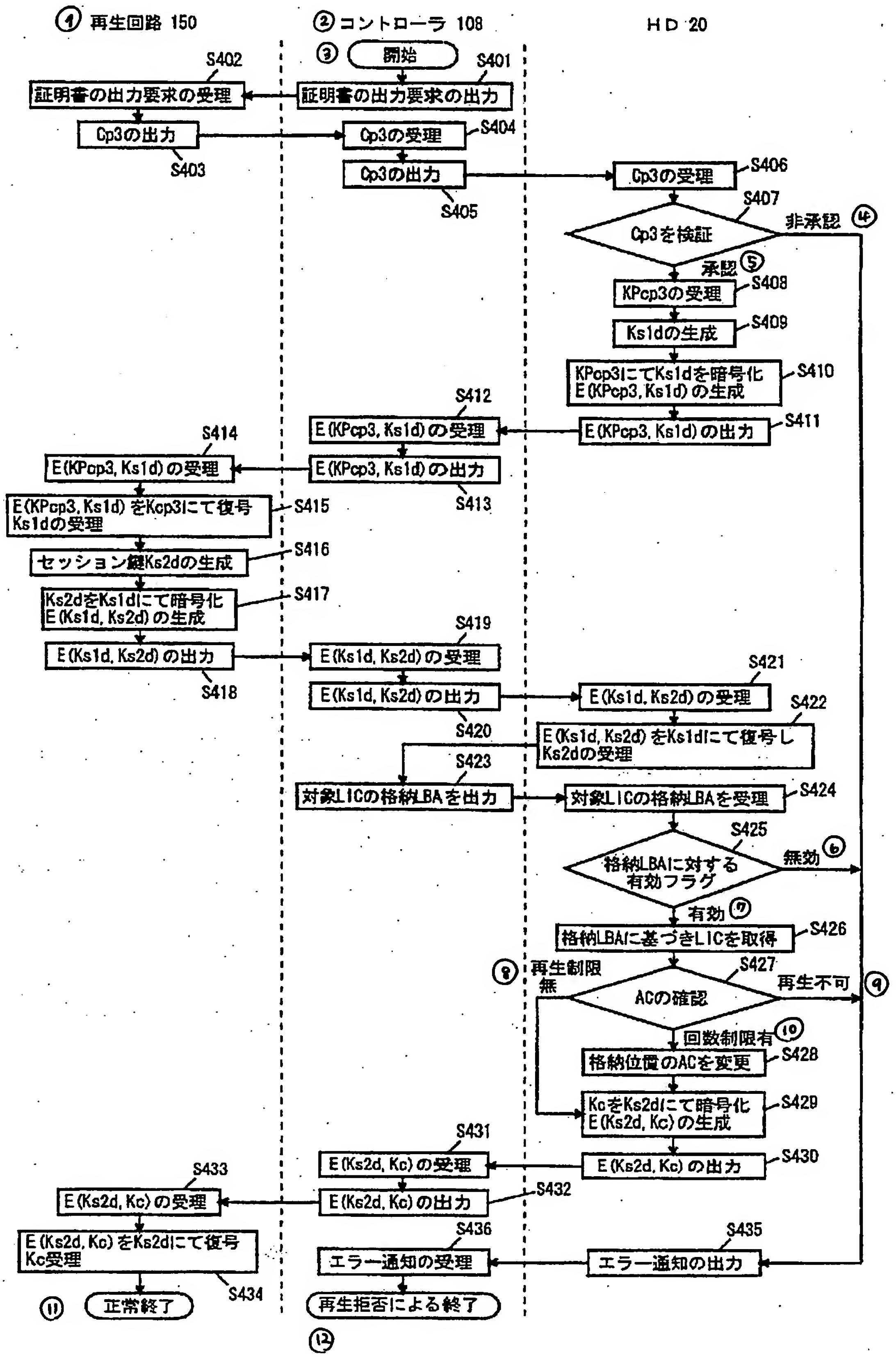
【図１７】


④
③
HD 20
端末装置 10
HD 21
S302から
② S322から
LID//E(Ks1b, Ks2c)//ST1//ST2 //E(Ks1b, H(LID//E(Ks1b, Ks2c)//ST1//ST2))の受理
S323
LID//E(Ks1b, Ks2c)//ST1//ST2 //E(Ks1b, H(LID//E(Ks1b, Ks2c)//ST1//ST2))の出力
S324
LID//E(Ks1b, Ks2c)//ST1//ST2 //E(Ks1b, H(LID//E(Ks1b, Ks2c)//ST1//ST2))の受理
S325
④
非承認
LID//E(Ks1b, Ks2c) //ST1//ST2//E(Ks1b, H(LID// E(Ks1b, Ks2c)//ST1//ST2)) を検証
S326
⑥
不一致
⑤ 承認
S327
LIDの確認
⑦ 一致
E(Ks1b, Ks2c)をKs1bにて復号し Ks2cの受理
S328
⑧
不一致
S329
Ks2a : Ks2c
⑨ 一致
⑩
受理済
S330
受信した ST1, ST2の確認
⑪ 非受理
⑫
不一致
ログメモリ に格納されたLBAに 記憶されるデータのLIDとログ メモリに格納された LIDの一致
S331
⑬ 一致
S332
⑭
有効
ログメモリ に格納されたLBAに対する 有効フラグ
⑮ 無効
S333
検索したライセンスを有効化
S335
ログメモリのLBAの出力
LBAの受理
S334
S336
セッション鍵要求の出力
セッション鍵Ks2bの作成
S337
再書込処理の対象 ⑯
S338
ログメモリにLIDとKs2bを格納し、 ST1を"受信待"に変更
Ks2bとKPom5をKs1bにて暗号化 E(Ks1b, Ks2b//KPom5)の生成
S339
S341
LID//E(Ks1b, Ks2b//KPom5) の受理
LID//E(Ks1b, Ks2b//KPom5)の出力
S340
LID//E(Ks1b, Ks2b//KPom5) の出力
S342
LID//E(Ks1b, Ks2b//KPom5)の受理
S343
E(Ks1b, Ks2b//KPom5)をKs1bにて復号し Ks2bとKPom5の受理
S344
⑰ S371へ
⑱ S345へ

【図１８】


② S302, S326, S327
S329～S331から
HD 20
S344から③
① 端末装置 10
HD 21
S345
ログメモリにLIDとKs2bとを格納し、ST1を"送信待"に変更
S346
対象LICの格納LBAを出力
対象LICの格納LBAを受理
S347
ログメモリにLBAを記憶
S348
④ 再書込処理の対象
⑤ 無効
格納LBAに対する有効フラグ
S349
⑥ 有効
LBAに基づきLICを取得
S350
⑦ 不一致
LIDの一致
S351
⑧ 一致
⑨ 禁止
ACの確認
S352
LICをKPom5にて暗号化
E(KPom5, LIC)の生成
S353
E(KPom5, LIC)をKs2bにて暗号化
E(Ks2b, E(KPom5, LIC))の生成
S354
⑩ 複製
ACの確認
S355
⑪ 移動
LBAに対する有効フラグを無効に変更
S356
ログメモリのST1を"送信済"に変更
S357
E(Ks2b, E(KPom5, LIC))の出力
S358
S359
E(Ks2b, E(KPom5, LIC))の受理
E(Ks2b, E(KPom5, LIC))の出力
S360
S361
E(Ks2b, E(KPom5, LIC))の受理
S362
E(Ks2b, E(KPom5, LIC))をKs2bにて復号
E(KPom5, LIC)の受理
S363
E(KPom5, LIC)をKom5にて復号
LICの受理
S364
LICの格納先LBAを出力
LICの格納先LBAを受理
S365
S366
ログメモリに格納先LBAを記録
S367
LIDの一致
一致 ⑫
不一致 ⑬
S372
エラー通知の出力
S373
エラー通知の受理
エラー通知の出力
S371
S368
書込拒否による終了
⑭
格納先LBAにLICを記録
格納先LBAに対する有効フラグを有効に変更
S369
ログメモリのST1を"受信済"に変更
S370
⑮ 正常終了

【図１９】


① 再生回路 150
② コントローラ 108
HD 20
③ 開始
S401
証明書の出力要求の出力
S402
証明書の出力要求の受理
Cp3の出力
S403
Cp3の受理
S404
Cp3の出力
S405
Cp3の受理
S406
S407
Cp3を検証
非承認 ④
承認 ⑤
KPcp3の受理
S408
Ks1dの生成
S409
KPcp3にてKs1dを暗号化
E(KPcp3, Ks1d)の生成
S410
E(KPcp3, Ks1d)の出力
S411
S412
E(KPcp3, Ks1d)の受理
E(KPcp3, Ks1d)の出力
S413
S414
E(KPcp3, Ks1d)の受理
E(KPcp3, Ks1d)をKcp3にて復号
Ks1dの受理
S415
セッション鍵Ks2dの生成
S416
Ks2dをKs1dにて暗号化
E(Ks1d, Ks2d)の生成
S417
E(Ks1d, Ks2d)の出力
S418
S419
E(Ks1d, Ks2d)の受理
E(Ks1d, Ks2d)の出力
S420
S421
E(Ks1d, Ks2d)の受理
S422
E(Ks1d, Ks2d)をKs1dにて復号し
Ks2dの受理
S423
対象LICの格納LBAを出力
対象LICの格納LBAを受理
S424
S425
格納LBAに対する
有効フラグ
無効 ⑥
有効 ⑦
格納LBAに基づきLICを取得
S426
⑧ 再生制限無
S427
ACの確認
再生不可 ⑨
回数制限有 ⑩
格納位置のACを変更
S428
KcをKs2dにて暗号化
E(Ks2d, Kc)の生成
S429
E(Ks2d, Kc)の出力
S430
S431
E(Ks2d, Kc)の受理
E(Ks2d, Kc)の出力
S432
S433
E(Ks2d, Kc)の受理
E(Ks2d, Kc)をKs2dにて復号
Kc受理
S434
⑪ 正常終了
S436
エラー通知の受理
S435
エラー通知の出力
再生拒否による終了
⑫

[Document Name] Abstract

[Abstract]

[Subject] A data recording device is provided that can rapidly specify a license being transmitted among a large number of recorded licenses, and particularly can achieve both of protection of the license and rapid reprocessing thereof in the case where a failure occurs while the license is being transmitted.

[Solving Means] A controller 214 in an HD (hard disk) 20, 21 serving as a data recording device stores a license including a content key for example for decrypting encrypted content data in a secure data storage portion 250. The license is managed by LBA (address information) in the secure data storage portion 250, and LBA where a license being transmitted is stored is stored as a log in a log memory in the secure data storage portion 250. When a failure occurs during the transmission process, the license being transmitted is specified based on the LBA stored in the log memory.

[Selected Drawing] Fig. 6